We have to ***watch and listen to everything that people are doing*** *so that we can catch terrorists, drug dealers, pedophiles, and organized criminals. Some of this data is sent unencrypted through the Internet, or sent encrypted to a company that passes the data along to us, but we learn much more when we have* ***comprehensive direct access to hundreds of millions of disks and screens and microphones and cameras****.*

This talk explains how we've successfully manipulated the world's software ecosystem to ensure our continuing access to this wealth of data. This talk will not cover our efforts against encryption, and will not cover our hardware back doors.

Making sure software stays insecure

Daniel J. Bernstein

University of Illinois at Chicago &
Technische Universiteit Eindhoven

e to ***watch and listen***
ything that people
ng *so that we can*
rrorists, drug dealers,
les, and organized
s. Some of this data
nencrypted through
rnet, or sent encrypted
npany that passes the
ng to us, but we learn
ore when we have
hensive direct access
lreds of millions of disks
eens and microphones
meras*.*

This talk explains how we've successfully manipulated the world's software ecosystem to ensure our continuing access to this wealth of data. This talk will not cover our efforts against encryption, and will not cover our hardware back doors.

Making sure
software stays insecure

Daniel J. Bernstein

University of Illinois at Chicago &
Technische Universiteit Eindhoven

Some im

1. *"We'*

I want s

h and listen
at people
we can
rug dealers,
rganized
f this data
d through
nt encrypted
t passes the
but we learn
we have
irect access
illions of disks
microphones

This talk explains how we've successfully manipulated the world's software ecosystem to ensure our continuing access to this wealth of data. This talk will not cover our efforts against encryption, and will not cover our hardware back doors.

Making sure
software stays insecure

Daniel J. Bernstein

University of Illinois at Chicago &
Technische Universiteit Eindhoven

Some important c

1. *"We"* doesn't i

I want secure softw

en

s,

a

ted

ne

rn

ess

disks

nes

This talk explains how we've successfully manipulated the world's software ecosystem to ensure our continuing access to this wealth of data. This talk will not cover our efforts against encryption, and will not cover our hardware back doors.

Making sure
software stays insecure

Daniel J. Bernstein

University of Illinois at Chicago &
Technische Universiteit Eindhoven

Some important clarification

1. *"We"* doesn't include me

I want secure software.

This talk explains how we've successfully manipulated the world's software ecosystem to ensure our continuing access to this wealth of data. This talk will not cover our efforts against encryption, and will not cover our hardware back doors.

Making sure
software stays insecure

Daniel J. Bernstein

University of Illinois at Chicago &
Technische Universiteit Eindhoven

Some important clarifications:

1. *"We"* doesn't include me.

I want secure software.

This talk explains how we've successfully manipulated the world's software ecosystem to ensure our continuing access to this wealth of data. This talk will not cover our efforts against encryption, and will not cover our hardware back doors.

Making sure
software stays insecure

Daniel J. Bernstein

University of Illinois at Chicago &
Technische Universiteit Eindhoven

Some important clarifications:

1. *"We"* doesn't include me.
I want secure software.

2. Their actions violate
fundamental human rights.

This talk explains how we've successfully manipulated the world's software ecosystem to ensure our continuing access to this wealth of data. This talk will not cover our efforts against encryption, and will not cover our hardware back doors.

Making sure
software stays insecure

Daniel J. Bernstein

University of Illinois at Chicago &
Technische Universiteit Eindhoven

Some important clarifications:

1. *"We"* doesn't include me.
I want secure software.

2. Their actions violate
fundamental human rights.

3. I don't have evidence that
they've deliberately manipulated
the software ecosystem.

This talk explains how we've successfully manipulated the world's software ecosystem to ensure our continuing access to this wealth of data. This talk will not cover our efforts against encryption, and will not cover our hardware back doors.

Making sure software stays insecure

Daniel J. Bernstein

University of Illinois at Chicago &
Technische Universiteit Eindhoven

Some important clarifications:

1. *"We"* doesn't include me.
I want secure software.

2. Their actions violate fundamental human rights.

3. I don't have evidence that they've deliberately manipulated the software ecosystem.

This talk is actually
a thought experiment:
how *could* an attacker manipulate the ecosystem for insecurity?

k explains how we've
fully manipulated the
software ecosystem to
our continuing access to
lth of data. This talk
cover our efforts against
on, and will not cover our
e back doors.

---

sure
stays insecure

. Bernstein

ty of Illinois at Chicago &
che Universiteit Eindhoven

Some important clarifications:

1. *"We"* doesn't include me.
I want secure software.

2. Their actions violate
fundamental human rights.

3. I don't have evidence that
they've deliberately manipulated
the software ecosystem.

This talk is actually
a thought experiment:
how *could* an attacker manipulate
the ecosystem for insecurity?

Distract

Identify
can't pr
but that
be mark

Example

Divert a
resource
away fro

how we've
ulated the
cosystem to
uing access to
a. This talk
efforts against
ill not cover our
ors.

---

ecure

n

is at Chicago &
siteit Eindhoven

Some important clarifications:

1. *"We"* doesn't include me.
I want secure software.

2. Their actions violate
fundamental human rights.

3. I don't have evidence that
they've deliberately manipulated
the software ecosystem.

This talk is actually
a thought experiment:
how *could* an attacker manipulate
the ecosystem for insecurity?

Distract managers

Identify activities t
can't produce secu
but that can never
be marketed as "s

Example: virus sca

Divert attention, f
resources, etc. into
away from actual s

e
e
to
s to
lk
ainst
er our

---

ago &
hoven

Some important clarifications:

1. *"We"* doesn't include me.
I want secure software.

2. Their actions violate
fundamental human rights.

3. I don't have evidence that
they've deliberately manipulated
the software ecosystem.

This talk is actually
a thought experiment:
how *could* an attacker manipulate
the ecosystem for insecurity?

Distract managers, sysadmin

Identify activities that
can't produce secure softwa
but that can nevertheless
be marketed as "security".

Example: virus scanners.

Divert attention, funding, hu
resources, etc. into "security
away from actual security.

Some important clarifications:

1. *"We"* doesn't include me.
I want secure software.

2. Their actions violate
fundamental human rights.

3. I don't have evidence that
they've deliberately manipulated
the software ecosystem.

This talk is actually
a thought experiment:
how *could* an attacker manipulate
the ecosystem for insecurity?

Distract managers, sysadmins, etc.

Identify activities that
can't produce secure software
but that can nevertheless
be marketed as "security".

Example: virus scanners.

Divert attention, funding, human
resources, etc. into "security",
away from actual security.

Some important clarifications:

1. *"We"* doesn't include me.
I want secure software.

2. Their actions violate
fundamental human rights.

3. I don't have evidence that
they've deliberately manipulated
the software ecosystem.

This talk is actually
a thought experiment:
how *could* an attacker manipulate
the ecosystem for insecurity?

Distract managers, sysadmins, etc.

Identify activities that
can't produce secure software
but that can nevertheless
be marketed as "security".

Example: virus scanners.

Divert attention, funding, human
resources, etc. into "security",
away from actual security.

People naturally do this.
Attacker investment is magnified.
Attack discovery is unlikely.

nportant clarifications:

' doesn't include me.
ecure software.

r actions violate
ental human rights.

't have evidence that
deliberately manipulated
ware ecosystem.

k is actually
nt experiment:
ld an attacker manipulate
ystem for insecurity?

Distract managers, sysadmins, etc.

Identify activities that
can't produce secure software
but that can nevertheless
be marketed as "security".

Example: virus scanners.

Divert attention, funding, human
resources, etc. into "security",
away from actual security.

People naturally do this.
Attacker investment is magnified.
Attack discovery is unlikely.

2014 NI
improvin
cybersec

"Cyberse
the incre
and con
infrastru
the Nati
and pub
risk. . . .

larifications:

nclude me.

ware.

iolate
an rights.

idence that
y manipulated
stem.

ly
ent:
cker manipulate
insecurity?

Distract managers, sysadmins, etc.

Identify activities that
can't produce secure software
but that can nevertheless
be marketed as "security".

Example: virus scanners.

Divert attention, funding, human resources, etc. into "security", away from actual security.

People naturally do this.

Attacker investment is magnified.

Attack discovery is unlikely.

2014 NIST "Fram
improving critical
cybersecurity":

"Cybersecurity thr
the increased com
and connectivity o
infrastructure syst
the Nation's secur
and public safety a
risk. . . .

s:

.

t

ated

pulate

?

Distract managers, sysadmins, etc.

Identify activities that
can't produce secure software
but that can nevertheless
be marketed as "security".

Example: virus scanners.

Divert attention, funding, human resources, etc. into "security", away from actual security.

People naturally do this.

Attacker investment is magnified.
Attack discovery is unlikely.

2014 NIST "Framework for improving critical infrastruct cybersecurity":

"Cybersecurity threats explo the increased complexity and connectivity of critical infrastructure systems, placi the Nation's security, econor and public safety and health risk. . . .

Distract managers, sysadmins, etc.

Identify activities that
can't produce secure software
but that can nevertheless
be marketed as "security".

Example: virus scanners.

Divert attention, funding, human resources, etc. into "security", away from actual security.

People naturally do this.
Attacker investment is magnified.
Attack discovery is unlikely.

2014 NIST "Framework for improving critical infrastructure cybersecurity":

"Cybersecurity threats exploit the increased complexity and connectivity of critical infrastructure systems, placing the Nation's security, economy, and public safety and health at risk. ...

Distract managers, sysadmins, etc.

Identify activities that
can't produce secure software
but that can nevertheless
be marketed as "security".

Example: virus scanners.

Divert attention, funding, human resources, etc. into "security", away from actual security.

People naturally do this.
Attacker investment is magnified.
Attack discovery is unlikely.

2014 NIST "Framework for improving critical infrastructure cybersecurity":

"Cybersecurity threats exploit the increased complexity and connectivity of critical infrastructure systems, placing the Nation's security, economy, and public safety and health at risk. . . . The Framework focuses on using business drivers to guide cybersecurity activities and considering cybersecurity risks as part of the organization's risk management processes."

managers, sysadmins, etc.

activities that
oduce secure software
can nevertheless
eted as "security".

e: virus scanners.

ttention, funding, human
s, etc. into "security",
om actual security.

naturally do this.
r investment is magnified.
discovery is unlikely.

2014 NIST "Framework for improving critical infrastructure cybersecurity":

"Cybersecurity threats exploit the increased complexity and connectivity of critical infrastructure systems, placing the Nation's security, economy, and public safety and health at risk. . . . The Framework focuses on using business drivers to guide cybersecurity activities and considering cybersecurity risks as part of the organization's risk management processes."

"This ris
an organ
estimate
to achie
cost-effe

, sysadmins, etc.

that
ure software
rtheless
ecurity".

anners.

unding, human
o "security",
security.

do this.
nt is magnified.
s unlikely.

2014 NIST "Framework for improving critical infrastructure cybersecurity":

"Cybersecurity threats exploit the increased complexity and connectivity of critical infrastructure systems, placing the Nation's security, economy, and public safety and health at risk. . . . The Framework focuses on using business drivers to guide cybersecurity activities and considering cybersecurity risks as part of the organization's risk management processes."

"This risk-based a
an organization to
estimates (e.g., sta
to achieve cyberse
cost-effective, prio

ns, etc.

re

uman

y",

nified.

2014 NIST "Framework for improving critical infrastructure cybersecurity":

"Cybersecurity threats exploit the increased complexity and connectivity of critical infrastructure systems, placing the Nation's security, economy, and public safety and health at risk. . . . The Framework focuses on using business drivers to guide cybersecurity activities and considering cybersecurity risks as part of the organization's risk management processes."

"This risk-based approach e
an organization to gauge res
estimates (e.g., staffing, fun
to achieve cybersecurity goa
cost-effective, prioritized ma

2014 NIST "Framework for improving critical infrastructure cybersecurity":

"Cybersecurity threats exploit the increased complexity and connectivity of critical infrastructure systems, placing the Nation's security, economy, and public safety and health at risk. . . . The Framework focuses on using business drivers to guide cybersecurity activities and considering cybersecurity risks as part of the organization's risk management processes."

"This risk-based approach enables an organization to gauge resource estimates (e.g., staffing, funding) to achieve cybersecurity goals in a cost-effective, prioritized manner."

2014 NIST "Framework for improving critical infrastructure cybersecurity":

"Cybersecurity threats exploit the increased complexity and connectivity of critical infrastructure systems, placing the Nation's security, economy, and public safety and health at risk. . . . The Framework focuses on using business drivers to guide cybersecurity activities and considering cybersecurity risks as part of the organization's risk management processes."

"This risk-based approach enables an organization to gauge resource estimates (e.g., staffing, funding) to achieve cybersecurity goals in a cost-effective, prioritized manner."

- "Identify."
  e.g. inventory your PCs.

2014 NIST "Framework for improving critical infrastructure cybersecurity":

"Cybersecurity threats exploit the increased complexity and connectivity of critical infrastructure systems, placing the Nation's security, economy, and public safety and health at risk. . . . The Framework focuses on using business drivers to guide cybersecurity activities and considering cybersecurity risks as part of the organization's risk management processes."

"This risk-based approach enables an organization to gauge resource estimates (e.g., staffing, funding) to achieve cybersecurity goals in a cost-effective, prioritized manner."

- "Identify."
  e.g. inventory your PCs.
- "Protect."
  e.g. inventory your humans.

2014 NIST "Framework for improving critical infrastructure cybersecurity":

"Cybersecurity threats exploit the increased complexity and connectivity of critical infrastructure systems, placing the Nation's security, economy, and public safety and health at risk. . . . The Framework focuses on using business drivers to guide cybersecurity activities and considering cybersecurity risks as part of the organization's risk management processes."

"This risk-based approach enables an organization to gauge resource estimates (e.g., staffing, funding) to achieve cybersecurity goals in a cost-effective, prioritized manner."

- "Identify."
  e.g. inventory your PCs.
- "Protect."
  e.g. inventory your humans.
- "Detect."
  e.g. install an IDS.

2014 NIST "Framework for improving critical infrastructure cybersecurity":

"Cybersecurity threats exploit the increased complexity and connectivity of critical infrastructure systems, placing the Nation's security, economy, and public safety and health at risk. . . . The Framework focuses on using business drivers to guide cybersecurity activities and considering cybersecurity risks as part of the organization's risk management processes."

"This risk-based approach enables an organization to gauge resource estimates (e.g., staffing, funding) to achieve cybersecurity goals in a cost-effective, prioritized manner."

- "Identify."
  e.g. inventory your PCs.
- "Protect."
  e.g. inventory your humans.
- "Detect."
  e.g. install an IDS.
- "Respond."
  e.g. coordinate with CERT.

2014 NIST "Framework for improving critical infrastructure cybersecurity":

"Cybersecurity threats exploit the increased complexity and connectivity of critical infrastructure systems, placing the Nation's security, economy, and public safety and health at risk. . . . The Framework focuses on using business drivers to guide cybersecurity activities and considering cybersecurity risks as part of the organization's risk management processes."

"This risk-based approach enables an organization to gauge resource estimates (e.g., staffing, funding) to achieve cybersecurity goals in a cost-effective, prioritized manner."

- "Identify."
  e.g. inventory your PCs.
- "Protect."
  e.g. inventory your humans.
- "Detect."
  e.g. install an IDS.
- "Respond."
  e.g. coordinate with CERT.
- "Recover."
  e.g. "Reputation is repaired."

ST "Framework for
ng critical infrastructure
curity":

ecurity threats exploit
eased complexity
nectivity of critical
cture systems, placing
on's security, economy,
lic safety and health at
The Framework focuses
g business drivers to
bersecurity activities and
ing cybersecurity risks
of the organization's risk
ment processes."

"This risk-based approach enables an organization to gauge resource estimates (e.g., staffing, funding) to achieve cybersecurity goals in a cost-effective, prioritized manner."

- "Identify."
  e.g. inventory your PCs.
- "Protect."
  e.g. inventory your humans.
- "Detect."
  e.g. install an IDS.
- "Respond."
  e.g. coordinate with CERT.
- "Recover."
  e.g. "Reputation is repaired."

Categori

- "Acces
- "Awar
- "Data
  e.g. in
- "Infor
  Proces
  e.g. in
- "Main
- "Prote
  e.g. re

ework for
infrastructure

reats exploit
plexity
f critical
ems, placing
ity, economy,
and health at
nework focuses
drivers to
y activities and
ecurity risks
anization's risk
esses."

"This risk-based approach enables an organization to gauge resource estimates (e.g., staffing, funding) to achieve cybersecurity goals in a cost-effective, prioritized manner."

- "Identify."
  e.g. inventory your PCs.
- "Protect."
  e.g. inventory your humans.
- "Detect."
  e.g. install an IDS.
- "Respond."
  e.g. coordinate with CERT.
- "Recover."
  e.g. "Reputation is repaired."

Categories inside "

- "Access Control
- "Awareness and
- "Data Security"
  e.g. inventory yo
- "Information Pro
  Processes and P
  e.g. inventory yo
- "Maintenance".
- "Protective Tech
  e.g. review your

ture

it

ng
my,
at
cuses

s and
ks
risk

"This risk-based approach enables an organization to gauge resource estimates (e.g., staffing, funding) to achieve cybersecurity goals in a cost-effective, prioritized manner."

- "Identify."
  e.g. inventory your PCs.
- "Protect."
  e.g. inventory your humans.
- "Detect."
  e.g. install an IDS.
- "Respond."
  e.g. coordinate with CERT.
- "Recover."
  e.g. "Reputation is repaired."

Categories inside "Protect":

- "Access Control".
- "Awareness and Training"
- "Data Security".
  e.g. inventory your data.
- "Information Protection
  Processes and Procedures"
  e.g. inventory your OS ver
- "Maintenance".
- "Protective Technology".
  e.g. review your audit logs

"This risk-based approach enables an organization to gauge resource estimates (e.g., staffing, funding) to achieve cybersecurity goals in a cost-effective, prioritized manner."

- "Identify."
  e.g. inventory your PCs.
- "Protect."
  e.g. inventory your humans.
- "Detect."
  e.g. install an IDS.
- "Respond."
  e.g. coordinate with CERT.
- "Recover."
  e.g. "Reputation is repaired."

Categories inside "Protect":

- "Access Control".
- "Awareness and Training".
- "Data Security".
  e.g. inventory your data.
- "Information Protection Processes and Procedures".
  e.g. inventory your OS versions.
- "Maintenance".
- "Protective Technology".
  e.g. review your audit logs.

"This risk-based approach enables an organization to gauge resource estimates (e.g., staffing, funding) to achieve cybersecurity goals in a cost-effective, prioritized manner."

- "Identify."
  e.g. inventory your PCs.
- "Protect."
  e.g. inventory your humans.
- "Detect."
  e.g. install an IDS.
- "Respond."
  e.g. coordinate with CERT.
- "Recover."
  e.g. "Reputation is repaired."

Categories inside "Protect":

- "Access Control".
- "Awareness and Training".
- "Data Security".
  e.g. inventory your data.
- "Information Protection Processes and Procedures".
  e.g. inventory your OS versions.
- "Maintenance".
- "Protective Technology".
  e.g. review your audit logs.

Subcategories in Framework: 98.

... promoting secure software: 0.

"This risk-based approach enables an organization to gauge resource estimates (e.g., staffing, funding) to achieve cybersecurity goals in a cost-effective, prioritized manner."

- "Identify."
  e.g. inventory your PCs.
- "Protect."
  e.g. inventory your humans.
- "Detect."
  e.g. install an IDS.
- "Respond."
  e.g. coordinate with CERT.
- "Recover."
  e.g. "Reputation is repaired."

Categories inside "Protect":

- "Access Control".
- "Awareness and Training".
- "Data Security".
  e.g. inventory your data.
- "Information Protection Processes and Procedures".
  e.g. inventory your OS versions.
- "Maintenance".
- "Protective Technology".
  e.g. review your audit logs.

Subcategories in Framework: 98.

... promoting secure software: 0.

This is how the money is spent.

sk-based approach enables
nization to gauge resource
es (e.g., staffing, funding)
ve cybersecurity goals in a
ective, prioritized manner."

ify."
ventory your PCs.
ect."
ventory your humans.
ct."
stall an IDS.
ond."
oordinate with CERT.
ver."
Reputation is repaired."

Categories inside "Protect":

- "Access Control".
- "Awareness and Training".
- "Data Security".
  e.g. inventory your data.
- "Information Protection Processes and Procedures".
  e.g. inventory your OS versions.
- "Maintenance".
- "Protective Technology".
  e.g. review your audit logs.

Subcategories in Framework: 98.

... promoting secure software: 0.

This is how the money is spent.

Distract

e.g. "Do
applicati
sources

e.g. "Be
links or
email or

e.g. "Im
suspect
to your
authoriti

e.g. "Ide
separate
personal

pproach enables
gauge resource
affing, funding)
curity goals in a
ritized manner."

our PCs.

our humans.

OS.

with CERT.

n is repaired."

Categories inside "Protect":

- "Access Control".
- "Awareness and Training".
- "Data Security".
  e.g. inventory your data.
- "Information Protection Processes and Procedures".
  e.g. inventory your OS versions.
- "Maintenance".
- "Protective Technology".
  e.g. review your audit logs.

Subcategories in Framework: 98.

... promoting secure software: 0.

This is how the money is spent.

<u>Distract users</u>

e.g. "Download or
applications from
sources or marketp

e.g. "Be suspicious
links or requests se
email or text mess

e.g. "Immediately
suspect data or se
to your supervisor
authorities."

e.g. "Ideally, you w
separate computer
personal use."

nables
source
ding)
ls in a
nner."

s.

T.

ed."

Categories inside "Protect":

- "Access Control".
- "Awareness and Training".
- "Data Security".
  e.g. inventory your data.
- "Information Protection Processes and Procedures".
  e.g. inventory your OS versions.
- "Maintenance".
- "Protective Technology".
  e.g. review your audit logs.

Subcategories in Framework: 98.

... promoting secure software: 0.

This is how the money is spent.

<u>Distract users</u>

e.g. "Download only trusted
applications from reputable
sources or marketplaces."

e.g. "Be suspicious of unkno
links or requests sent throug
email or text message."

e.g. "Immediately report any
suspect data or security brea
to your supervisor and/or
authorities."

e.g. "Ideally, you will have
separate computers for work
personal use."

Categories inside “Protect”:

- “Access Control”.
- “Awareness and Training”.
- “Data Security”.
  e.g. inventory your data.
- “Information Protection Processes and Procedures”.
  e.g. inventory your OS versions.
- “Maintenance”.
- “Protective Technology”.
  e.g. review your audit logs.

Subcategories in Framework: 98.

. . . promoting secure software: 0.

This is how the money is spent.

Distract users

e.g. “Download only trusted applications from reputable sources or marketplaces.”

e.g. “Be suspicious of unknown links or requests sent through email or text message.”

e.g. “Immediately report any suspect data or security breaches to your supervisor and/or authorities.”

e.g. “Ideally, you will have separate computers for work and personal use.”

es inside “Protect”:
ss Control”.
eness and Training”.
Security”.
ventory your data.
mation Protection
sses and Procedures”.
ventory your OS versions.
tenance”.
ective Technology”.
view your audit logs.

gories in Framework: 98.
noting secure software: 0.

how the money is spent.

Distract users

e.g. “Download only trusted applications from reputable sources or marketplaces.”

e.g. “Be suspicious of unknown links or requests sent through email or text message.”

e.g. “Immediately report any suspect data or security breaches to your supervisor and/or authorities.”

e.g. “Ideally, you will have separate computers for work and personal use.”

Distract

Example
software

“Protect”:
”.
Training”.
.
our data.
otection
rocedures”.
our OS versions.

nology”.
audit logs.

Framework: 98.
ure software: 0.

money is spent.

Distract users

e.g. “Download only trusted applications from reputable sources or marketplaces.”

e.g. “Be suspicious of unknown links or requests sent through email or text message.”

e.g. “Immediately report any suspect data or security breaches to your supervisor and/or authorities.”

e.g. “Ideally, you will have separate computers for work and personal use.”

Distract programm

Example: automat
software “security”

.

’.

rsions.

s.

: 98.

re: 0.

spent.

Distract users

e.g. “Download only trusted applications from reputable sources or marketplaces.”

e.g. “Be suspicious of unknown links or requests sent through email or text message.”

e.g. “Immediately report any suspect data or security breaches to your supervisor and/or authorities.”

e.g. “Ideally, you will have separate computers for work and personal use.”

Distract programmers

Example: automatic low-lat
software “security” updates.

Distract users

e.g. “Download only trusted applications from reputable sources or marketplaces.”

e.g. “Be suspicious of unknown links or requests sent through email or text message.”

e.g. “Immediately report any suspect data or security breaches to your supervisor and/or authorities.”

e.g. “Ideally, you will have separate computers for work and personal use.”

Distract programmers

Example: automatic low-latency software “security” updates.

Distract users

e.g. “Download only trusted applications from reputable sources or marketplaces.”

e.g. “Be suspicious of unknown links or requests sent through email or text message.”

e.g. “Immediately report any suspect data or security breaches to your supervisor and/or authorities.”

e.g. “Ideally, you will have separate computers for work and personal use.”

Distract programmers

Example: automatic low-latency software “security” updates.

Marketing: “security” is defined by *public security holes*.
Known hole in Product 2014.06?
Update now to Product 2014.07!

Distract users

e.g. “Download only trusted applications from reputable sources or marketplaces.”

e.g. “Be suspicious of unknown links or requests sent through email or text message.”

e.g. “Immediately report any suspect data or security breaches to your supervisor and/or authorities.”

e.g. “Ideally, you will have separate computers for work and personal use.”

Distract programmers

Example: automatic low-latency software “security” updates.

Marketing: “security” is defined by *public security holes*.
Known hole in Product 2014.06?
Update now to Product 2014.07!

To help the marketing, publicize actual attacks that exploit public security holes.

Distract users

e.g. “Download only trusted applications from reputable sources or marketplaces.”

e.g. “Be suspicious of unknown links or requests sent through email or text message.”

e.g. “Immediately report any suspect data or security breaches to your supervisor and/or authorities.”

e.g. “Ideally, you will have separate computers for work and personal use.”

Distract programmers

Example: automatic low-latency software “security” updates.

Marketing: “security” is defined by *public security holes*.
Known hole in Product 2014.06?
Update now to Product 2014.07!

To help the marketing, publicize actual attacks that exploit public security holes.

Reality: Product 2014.07 also has security holes that attackers are exploiting.

users

ownload only trusted
ions from reputable
or marketplaces."

suspicious of unknown
requests sent through
text message."

mediately report any
data or security breaches
supervisor and/or
ies."

eally, you will have
computers for work and
use."

Distract programmers

Example: automatic low-latency software "security" updates.

Marketing: "security" is defined by *public security holes*.
Known hole in Product 2014.06?
Update now to Product 2014.07!

To help the marketing, publicize actual attacks that exploit public security holes.

Reality: Product 2014.07 also has security holes that attackers are exploiting.

Distract

Example
When re
showing
create a
the amo

"You co

"How m

"Do you
to use 1
just to b

nly trusted
reputable
places."

s of unknown
ent through
sage."

report any
curity breaches
and/or

will have
rs for work and

Distract programmers

Example: automatic low-latency software "security" updates.

Marketing: "security" is defined by *public security holes*.
Known hole in Product 2014.06?
Update now to Product 2014.07!

To help the marketing,
publicize actual attacks that
exploit public security holes.

Reality: Product 2014.07
also has security holes
that attackers are exploiting.

Distract researcher

Example:
When researcher f
showing that a sys
create a competiti
the amount of dar

"You corrupted on

"How many users

"Do you really exp
to use 100 CPU co
just to break this s

own
gh

y
aches

k and

Distract programmers

Example: automatic low-latency software "security" updates.

Marketing: "security" is defined by *public security holes*.
Known hole in Product 2014.06?
Update now to Product 2014.07!

To help the marketing, publicize actual attacks that exploit public security holes.

Reality: Product 2014.07 also has security holes that attackers are exploiting.

Distract researchers

Example:
When researcher finds attac
showing that a system is ins
create a competition for
the amount of damage.

"You corrupted only one file

"How many users are affecte

"Do you really expect an att
to use 100 CPU cores for a
just to break this system?"

Distract programmers

Example: automatic low-latency software "security" updates.

Marketing: "security" is defined by *public security holes*.
Known hole in Product 2014.06?
Update now to Product 2014.07!

To help the marketing,
publicize actual attacks that exploit public security holes.

Reality: Product 2014.07
also has security holes
that attackers are exploiting.

Distract researchers

Example:
When researcher finds attack showing that a system is insecure, create a competition for *the amount of damage*.

"You corrupted only one file?"

"How many users are affected?"

"Do you really expect an attacker to use 100 CPU cores for a month just to break this system?"

Distract programmers

Example: automatic low-latency software "security" updates.

Marketing: "security" is defined by *public security holes*.
Known hole in Product 2014.06?
Update now to Product 2014.07!

To help the marketing,
publicize actual attacks that exploit public security holes.

Reality: Product 2014.07
also has security holes
that attackers are exploiting.

Distract researchers

Example:
When researcher finds attack showing that a system is insecure, create a competition for *the amount of damage*.

"You corrupted only one file?"

"How many users are affected?"

"Do you really expect an attacker to use 100 CPU cores for a month just to break this system?"

⇒ More attack papers!

programmers

e: automatic low-latency
"security" updates.

ng: "security" is defined
c security holes.
hole in Product 2014.06?
now to Product 2014.07!

the marketing,
e actual attacks that
ublic security holes.

Product 2014.07
security holes
ackers are exploiting.

Distract researchers

Example:
When researcher finds attack
showing that a system is insecure,
create a competition for
the amount of damage.

"You corrupted only one file?"

"How many users are affected?"

"Do you really expect an attacker
to use 100 CPU cores for a month
just to break this system?"

⇒ More attack papers!

Discoura

Tell prog
"100% s
so they

ners

tic low-latency
" updates.

ity" is defined
holes.
oduct 2014.06?
oduct 2014.07!

eting,
tacks that
urity holes.

2014.07
oles
exploiting.

Distract researchers

Example:
When researcher finds attack
showing that a system is insecure,
create a competition for
the amount of damage.

"You corrupted only one file?"

"How many users are affected?"

"Do you really expect an attacker
to use 100 CPU cores for a month
just to break this system?"

⇒ More attack papers!

Discourage securit

Tell programmers
"100% security is
so they shouldn't

ency

ined

4.06?

4.07!

Distract researchers

Example:
When researcher finds attack
showing that a system is insecure,
create a competition for
the amount of damage.

"You corrupted only one file?"

"How many users are affected?"

"Do you really expect an attacker
to use 100 CPU cores for a month
just to break this system?"

⇒ More attack papers!

Discourage security

Tell programmers that
"100% security is impossible"
so they shouldn't even try.

Distract researchers

Example:
When researcher finds attack
showing that a system is insecure,
create a competition for
the amount of damage.

"You corrupted only one file?"

"How many users are affected?"

"Do you really expect an attacker
to use 100 CPU cores for a month
just to break this system?"

$\Rightarrow$ More attack papers!

Discourage security

Tell programmers that
"100% security is impossible"
so they shouldn't even try.

Distract researchers

Example:
When researcher finds attack
showing that a system is insecure,
create a competition for
the amount of damage.

"You corrupted only one file?"

"How many users are affected?"

"Do you really expect an attacker
to use 100 CPU cores for a month
just to break this system?"

⇒ More attack papers!

Discourage security

Tell programmers that
"100% security is impossible"
so they shouldn't even try.

Tell programmers that
"defining security is impossible"
so it can't be implemented.

Distract researchers

Example:
When researcher finds attack
showing that a system is insecure,
create a competition for
the amount of damage.

"You corrupted only one file?"

"How many users are affected?"

"Do you really expect an attacker
to use 100 CPU cores for a month
just to break this system?"

⇒ More attack papers!

Discourage security

Tell programmers that
"100% security is impossible"
so they shouldn't even try.

Tell programmers that
"defining security is impossible"
so it can't be implemented.

Hide/dismiss/mismeasure
security metric #1.

Distract researchers

Example:
When researcher finds attack
showing that a system is insecure,
create a competition for
the amount of damage.

"You corrupted only one file?"

"How many users are affected?"

"Do you really expect an attacker
to use 100 CPU cores for a month
just to break this system?"

⇒ More attack papers!

Discourage security

Tell programmers that
"100% security is impossible"
so they shouldn't even try.

Tell programmers that
"defining security is impossible"
so it can't be implemented.

Hide/dismiss/mismeasure
security metric #1.

Prioritize compatibility,
"standards", speed, etc. e.g.:
"An HTTP server in the kernel
is critical for performance."

researchers

e:

esearcher finds attack

that a system is insecure,

competition for

unt of damage.

rrupted only one file?"

any users are affected?"

really expect an attacker

00 CPU cores for a month

break this system?"

attack papers!

Discourage security

Tell programmers that

"100% security is impossible"

so they shouldn't even try.

Tell programmers that

"defining security is impossible"

so it can't be implemented.

Hide/dismiss/mismeasure

security metric #1.

Prioritize compatibility,

"standards", speed, etc. e.g.:

"An HTTP server in the kernel

is critical for performance."

What is

Integrity

Whenev

shows m

it also te

the sour

e.g. If E

and con

to show

as havin

then this

I have a

security

but this

rs

inds attack
stem is insecure,
on for
mage.

ly one file?"

are affected?"

pect an attacker
ores for a month
system?"

apers!

Discourage security

Tell programmers that
"100% security is impossible"
so they shouldn't even try.

Tell programmers that
"defining security is impossible"
so it can't be implemented.

Hide/dismiss/mismeasure
security metric #1.

Prioritize compatibility,
"standards", speed, etc. e.g.:
"An HTTP server in the kernel
is critical for performance."

What is security?

Integrity policy #1
Whenever the com
shows me a file,
it also tells me
the source of the f

e.g. If Eve creates
and convinces the
to show me the fil
as having source F
then this policy is

I have a few other
security policies,
but this is my top

k
ecure,

?"

ed?"

tacker
month

Discourage security

Tell programmers that
"100% security is impossible"
so they shouldn't even try.

Tell programmers that
"defining security is impossible"
so it can't be implemented.

Hide/dismiss/mismeasure
security metric #1.

Prioritize compatibility,
"standards", speed, etc. e.g.:
"An HTTP server in the kernel
is critical for performance."

What is security?

Integrity policy #1:
Whenever the computer
shows me a file,
it also tells me
the source of the file.

e.g. If Eve creates a file
and convinces the computer
to show me the file
as having source `Frank`
then this policy is violated.

I have a few other
security policies,
but this is my top priority.

Discourage security

Tell programmers that
"100% security is impossible"
so they shouldn't even try.

Tell programmers that
"defining security is impossible"
so it can't be implemented.

Hide/dismiss/mismeasure
security metric #1.

Prioritize compatibility,
"standards", speed, etc. e.g.:
"An HTTP server in the kernel
is critical for performance."

What is security?

Integrity policy #1:
Whenever the computer
shows me a file,
it also tells me
the source of the file.

e.g. If Eve creates a file
and convinces the computer
to show me the file
as having source `Frank`
then this policy is violated.

I have a few other
security policies,
but this is my top priority.

age security

grammers that
security is impossible"
shouldn't even try.

grammers that
g security is impossible"
n't be implemented.

smiss/mismeasure
metric #1.

e compatibility,
rds", speed, etc. e.g.:
TP server in the kernel
l for performance."

What is security?

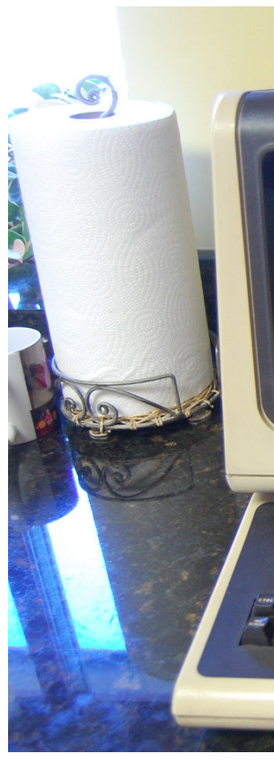
Integrity policy #1:
Whenever the computer
shows me a file,
it also tells me
the source of the file.

e.g. If Eve creates a file
and convinces the computer
to show me the file
as having source `Frank`
then this policy is violated.

I have a few other
security policies,
but this is my top priority.

The trus

1987: M
Low-cos
multi-us



Picture cr
terminal
/wiki/in

y

that
impossible"
even try.

that
is impossible"
lemented.

measure
l..

bility,
d, etc. e.g.:
in the kernel
ormance."

What is security?

Integrity policy #1:
Whenever the computer
shows me a file,
it also tells me
the source of the file.

e.g. If Eve creates a file
and convinces the computer
to show me the file
as having source `Frank`
then this policy is violated.

I have a few other
security policies,
but this is my top priority.

The trusted compu

1987: My first UN
Low-cost terminals
multi-user Ultrix c

Picture credit:
terminals.classicc
/wiki/index.php/DE

e"

ble"

..:

rnel

What is security?

Integrity policy #1:
Whenever the computer
shows me a file,
it also tells me
the source of the file.

e.g. If Eve creates a file
and convinces the computer
to show me the file
as having source `Frank`
then this policy is violated.

I have a few other
security policies,
but this is my top priority.

The trusted computing base

1987: My first UNIX experie
Low-cost terminals access
multi-user Ultrix computer.

Picture credit:
terminals.classiccmp.org
/wiki/index.php/DEC_VT102

What is security?

Integrity policy #1:
Whenever the computer
shows me a file,
it also tells me
the source of the file.

e.g. If Eve creates a file
and convinces the computer
to show me the file
as having source `Frank`
then this policy is violated.

I have a few other
security policies,
but this is my top priority.

The trusted computing base

1987: My first UNIX experience.
Low-cost terminals access
multi-user Ultrix computer.

Picture credit:
terminals.classiccmp.org
/wiki/index.php/DEC_VT102

security?

policy #1:
er the computer
ne a file,
ells me
ce of the file.

ve creates a file
vinces the computer
me the file
g source `Frank`
s policy is violated.

few other
policies,
is my top priority.

The trusted computing base

1987: My first UNIX experience.
Low-cost terminals access
multi-user Ultrix computer.

Picture credit:
terminals.classiccmp.org
/wiki/index.php/DEC_VT102

I log in t
store file
start pro

Eve logs
stores fil
starts pr

Frank lo
stores fil
starts pr

Eve and
store file
start pro
(Of cour

1:
nputer

file.

a file
computer
e
Frank
violated.

priority.

The trusted computing base

1987: My first UNIX experience.
Low-cost terminals access
multi-user Ultrix computer.

Picture credit:
terminals.classiccmp.org
/wiki/index.php/DEC_VT102

I log in to the Ultr
store files labeled
start processes lab

Eve logs in,
stores files labeled
starts processes la

Frank logs in,
stores files labeled
starts processes la

Eve and Frank can
store files labeled
start processes lab
(Of course, sysadm

The trusted computing base

1987: My first UNIX experience.
Low-cost terminals access
multi-user Ultrix computer.

Picture credit:
terminals.classiccmp.org
/wiki/index.php/DEC_VT102

I log in to the Ultrix comput
store files labeled `Dan`,
start processes labeled `Dan`.

Eve logs in,
stores files labeled `Eve`,
starts processes labeled `Eve`.

Frank logs in,
stores files labeled `Frank`,
starts processes labeled `Fra`

Eve and Frank cannot
store files labeled `Dan`,
start processes labeled `Dan`.
(Of course, sysadmin can.)

The trusted computing base

1987: My first UNIX experience.
Low-cost terminals access
multi-user Ultrix computer.

Picture credit:
terminals.classiccmp.org
/wiki/index.php/DEC_VT102

I log in to the Ultrix computer,
store files labeled `Dan`,
start processes labeled `Dan`.

Eve logs in,
stores files labeled `Eve`,
starts processes labeled `Eve`.

Frank logs in,
stores files labeled `Frank`,
starts processes labeled `Frank`.

Eve and Frank cannot
store files labeled `Dan`,
start processes labeled `Dan`.
(Of course, sysadmin can.)

sted computing base

My first UNIX experience.
t terminals access
er Ultrix computer.

edit:
s.classiccmp.org
dex.php/DEC_VT102

I log in to the Ultrix computer,
store files labeled `Dan`,
start processes labeled `Dan`.

Eve logs in,
stores files labeled `Eve`,
starts processes labeled `Eve`.

Frank logs in,
stores files labeled `Frank`,
starts processes labeled `Frank`.

Eve and Frank cannot
store files labeled `Dan`,
start processes labeled `Dan`.
(Of course, sysadmin can.)

How is t

OS kern

`Dan`
`Eve`
`Frank`

OS kern

`Dan`
`Eve`
`Frank`

uting base

NIX experience.

s access

omputer.

mp.org
C_VT102

I log in to the Ultrix computer,
store files labeled `Dan`,
start processes labeled `Dan`.

Eve logs in,
stores files labeled `Eve`,
starts processes labeled `Eve`.

Frank logs in,
stores files labeled `Frank`,
starts processes labeled `Frank`.

Eve and Frank cannot
store files labeled `Dan`,
start processes labeled `Dan`.
(Of course, sysadmin can.)

How is this implem

OS kernel allocate

	system fil
`Dan`	my files
`Eve`	Eve's files
`Frank`	Frank's fi

OS kernel allocate

	kernel me
`Dan`	my proces
`Eve`	Eve's proc
`Frank`	Frank's pr

ence.

I log in to the Ultrix computer,
store files labeled `Dan`,
start processes labeled `Dan`.

Eve logs in,
stores files labeled `Eve`,
starts processes labeled `Eve`.

Frank logs in,
stores files labeled `Frank`,
starts processes labeled `Frank`.

Eve and Frank cannot
store files labeled `Dan`,
start processes labeled `Dan`.
(Of course, sysadmin can.)

How is this implemented?

OS kernel allocates disk spa

	system files
`Dan`	my files
`Eve`	Eve's files
`Frank`	Frank's files

OS kernel allocates RAM:

	kernel memory
`Dan`	my processes
`Eve`	Eve's processes
`Frank`	Frank's processes

I log in to the Ultrix computer,
store files labeled `Dan`,
start processes labeled `Dan`.

Eve logs in,
stores files labeled `Eve`,
starts processes labeled `Eve`.

Frank logs in,
stores files labeled `Frank`,
starts processes labeled `Frank`.

Eve and Frank cannot
store files labeled `Dan`,
start processes labeled `Dan`.
(Of course, sysadmin can.)

How is this implemented?

OS kernel allocates disk space:

	system files
`Dan`	my files
`Eve`	Eve's files
`Frank`	Frank's files

OS kernel allocates RAM:

	kernel memory
`Dan`	my processes
`Eve`	Eve's processes
`Frank`	Frank's processes

to the Ultrix computer,
es labeled `Dan`,
ocesses labeled `Dan`.

in,
es labeled `Eve`,
ocesses labeled `Eve`.

gs in,
es labeled `Frank`,
ocesses labeled `Frank`.

Frank cannot
es labeled `Dan`,
ocesses labeled `Dan`.
rse, sysadmin can.)

How is this implemented?

OS kernel allocates disk space:

	system files
`Dan`	my files
`Eve`	Eve's files
`Frank`	Frank's files

OS kernel allocates RAM:

	kernel memory
`Dan`	my processes
`Eve`	Eve's processes
`Frank`	Frank's processes

CPU har
memory
a user p
read or w
or RAM
without

Kernel e

When a
process

Process
any file
but not

rix computer,
Dan,
eled Dan.

Eve,
beled Eve.

Frank,
beled Frank.

nnot
Dan,
eled Dan.
min can.)

How is this implemented?

OS kernel allocates disk space:

	system files
Dan	my files
Eve	Eve's files
Frank	Frank's files

OS kernel allocates RAM:

	kernel memory
Dan	my processes
Eve	Eve's processes
Frank	Frank's processes

CPU hardware enf
memory protecti
a user process can
read or write files
or RAM in other p
without permissio

Kernel enforces va

When a process cr
process or a file, k

Process is allowed
any file with the s
but not with differ

ter,

nk.

How is this implemented?

OS kernel allocates disk space:

	system files
`Dan`	my files
`Eve`	Eve's files
`Frank`	Frank's files

OS kernel allocates RAM:

	kernel memory
`Dan`	my processes
`Eve`	Eve's processes
`Frank`	Frank's processes

CPU hardware enforces
memory protection:
a user process cannot
read or write files
or RAM in other processes
without permission from ker

Kernel enforces various rules

When a process creates anot
process or a file, kernel copie

Process is allowed to read or
any file with the same uid,
but not with different uid.

How is this implemented?

OS kernel allocates disk space:

	system files
`Dan`	my files
`Eve`	Eve's files
`Frank`	Frank's files

OS kernel allocates RAM:

	kernel memory
`Dan`	my processes
`Eve`	Eve's processes
`Frank`	Frank's processes

CPU hardware enforces
memory protection:
a user process cannot
read or write files
or RAM in other processes
without permission from kernel.

Kernel enforces various rules.

When a process creates another
process or a file, kernel copies uid.

Process is allowed to read or write
any file with the same uid,
but not with different uid.

chis implemented?

el allocates disk space:

system files
my files
Eve's files
Frank's files

el allocates RAM:

kernel memory
my processes
Eve's processes
Frank's processes

CPU hardware enforces
memory protection:
a user process cannot
read or write files
or RAM in other processes
without permission from kernel.

Kernel enforces various rules.

When a process creates another
process or a file, kernel copies uid.

Process is allowed to read or write
any file with the same uid,
but not with different uid.

Assume
How do
Eve can'

1. Chec
enforces

mented?

s disk space:

es
s
les

s RAM:

emory
sses
cesses
rocesses

CPU hardware enforces
memory protection:
a user process cannot
read or write files
or RAM in other processes
without permission from kernel.

Kernel enforces various rules.

When a process creates another
process or a file, kernel copies uid.

Process is allowed to read or write
any file with the same uid,
but not with different uid.

Assume the hardw
How do we verify
Eve can't write Da

1. Check the code
enforces these rule

ce:

CPU hardware enforces
memory protection:
a user process cannot
read or write files
or RAM in other processes
without permission from kernel.

Kernel enforces various rules.

When a process creates another
process or a file, kernel copies uid.

Process is allowed to read or write
any file with the same uid,
but not with different uid.

Assume the hardware works.
How do we verify that
Eve can't write Dan's files?

1. Check the code that
enforces these rules.

CPU hardware enforces
memory protection:
a user process cannot
read or write files
or RAM in other processes
without permission from kernel.

Kernel enforces various rules.

When a process creates another
process or a file, kernel copies uid.

Process is allowed to read or write
any file with the same uid,
but not with different uid.

Assume the hardware works.
How do we verify that
Eve can't write Dan's files?

1. Check the code that
enforces these rules.

CPU hardware enforces
memory protection:
a user process cannot
read or write files
or RAM in other processes
without permission from kernel.

Kernel enforces various rules.

When a process creates another
process or a file, kernel copies uid.

Process is allowed to read or write
any file with the same uid,
but not with different uid.

Assume the hardware works.
How do we verify that
Eve can't write Dan's files?

1. Check the code that
enforces these rules.

2. Check the code that
allocates disk space, RAM;
and user-authentication code.

CPU hardware enforces
memory protection:
a user process cannot
read or write files
or RAM in other processes
without permission from kernel.

Kernel enforces various rules.

When a process creates another
process or a file, kernel copies uid.

Process is allowed to read or write
any file with the same uid,
but not with different uid.

Assume the hardware works.
How do we verify that
Eve can't write Dan's files?

1. Check the code that
enforces these rules.

2. Check the code that
allocates disk space, RAM;
and user-authentication code.

3. Check all other kernel code.
Bugs anywhere in kernel
can override these rules.
Memory protection doesn't apply;
language (C) doesn't compensate.

rdware enforces
y protection:
rocess cannot
write files
in other processes
permission from kernel.

nforces various rules.

process creates another
or a file, kernel copies uid.

is allowed to read or write
with the same uid,
with different uid.

Assume the hardware works.
How do we verify that
Eve can't write Dan's files?

1. Check the code that
enforces these rules.

2. Check the code that
allocates disk space, RAM;
and user-authentication code.

3. Check all other kernel code.

Bugs anywhere in kernel
can override these rules.
Memory protection doesn't apply;
language (C) doesn't compensate.

The cod
trusted
Security

Eve can'
unless th

Eve's ac
Other so
Millions
that we

Do we n
Keep co
Limit so

forces
on:
not

processes
n from kernel.

rious rules.

reates another
ernel copies uid.

to read or write
ame uid,
rent uid.

Assume the hardware works.
How do we verify that
Eve can't write Dan's files?

1. Check the code that
enforces these rules.

2. Check the code that
allocates disk space, RAM;
and user-authentication code.

3. Check all other kernel code.
Bugs anywhere in kernel
can override these rules.
Memory protection doesn't apply;
language (C) doesn't compensate.

The code we have
trusted computin
Security metric #

Eve can't write Da
unless there's a T

Eve's actions: irre
Other software: ir
Millions of lines of
that we *don't* hav

Do we need an au
Keep computers s
Limit software Eve

nel.

s.

ther

es uid.

r write

Assume the hardware works.
How do we verify that
Eve can't write Dan's files?

1. Check the code that
enforces these rules.

2. Check the code that
allocates disk space, RAM;
and user-authentication code.

3. Check all other kernel code.

Bugs anywhere in kernel
can override these rules.
Memory protection doesn't apply;
language (C) doesn't compensate.

The code we have to check
trusted computing base.
Security metric #1: TCB si

Eve can't write Dan's files
unless there's a TCB bug.

Eve's actions: irrelevant.
Other software: irrelevant.
Millions of lines of code
that we *don't* have to check

Do we need an audit log? N
Keep computers separate? N
Limit software Eve can run?

Assume the hardware works.
How do we verify that
Eve can't write Dan's files?

1. Check the code that
enforces these rules.

2. Check the code that
allocates disk space, RAM;
and user-authentication code.

3. Check all other kernel code.
Bugs anywhere in kernel
can override these rules.
Memory protection doesn't apply;
language (C) doesn't compensate.

The code we have to check is the
trusted computing base.
Security metric #1: TCB size.

Eve can't write Dan's files
unless there's a TCB bug.

Eve's actions: irrelevant.
Other software: irrelevant.
Millions of lines of code
that we *don't* have to check.

Do we need an audit log? No.
Keep computers separate? No.
Limit software Eve can run? No.

the hardware works.
we verify that
't write Dan's files?

k the code that
these rules.

k the code that
s disk space, RAM;
r-authentication code.

k all other kernel code.
ywhere in kernel
rride these rules.
protection doesn't apply;
e (C) doesn't compensate.

The code we have to check is the **trusted computing base**.
Security metric #1: TCB size.

Eve can't write Dan's files
unless there's a TCB bug.

Eve's actions: irrelevant.
Other software: irrelevant.
Millions of lines of code
that we *don't* have to check.

Do we need an audit log? No.
Keep computers separate? No.
Limit software Eve can run? No.

File shar

So far h
complete

But user
many of
consider

I want t
to mark
as reada
or also r
or to Ev
or to a b
or to the

vare works.
that
an's files?

e that
es.

e that
ce, RAM;
cation code.

kernel code.
kernel
rules.
n doesn't apply;
sn't compensate.

The code we have to check is the **trusted computing base**.
Security metric #1: TCB size.

Eve can't write Dan's files
unless there's a TCB bug.

Eve's actions: irrelevant.
Other software: irrelevant.
Millions of lines of code
that we *don't* have to check.

Do we need an audit log? No.
Keep computers separate? No.
Limit software Eve can run? No.

File sharing

So far have descril
complete user isol

But users want to
many of their files
consider the Web,

I want to be able
to mark a file I ow
as readable to just
or also readable to
or to Eve+Frank;
or to a bigger grou
or to the general p

e.

de.

apply;

ensate.

The code we have to check is the **trusted computing base**.
Security metric #1: TCB size.

Eve can't write Dan's files
unless there's a TCB bug.

Eve's actions: irrelevant.
Other software: irrelevant.
Millions of lines of code
that we *don't* have to check.

Do we need an audit log? No.
Keep computers separate? No.
Limit software Eve can run? No.

File sharing

So far have described
complete user isolation.

But users want to share
many of their files:
consider the Web, email, etc

I want to be able
to mark a file I own
as readable to just me;
or also readable to Frank;
or to Eve+Frank;
or to a bigger group;
or to the general public.

The code we have to check is the
trusted computing base.
Security metric #1: TCB size.

Eve can't write Dan's files
unless there's a TCB bug.

Eve's actions: irrelevant.
Other software: irrelevant.
Millions of lines of code
that we *don't* have to check.

Do we need an audit log? No.
Keep computers separate? No.
Limit software Eve can run? No.

File sharing

So far have described
complete user isolation.

But users want to share
many of their files:
consider the Web, email, etc.

I want to be able
to mark a file I own
as readable to just me;
or also readable to Frank;
or to Eve+Frank;
or to a bigger group;
or to the general public.

e we have to check is the
computing base.
metric #1: TCB size.

't write Dan's files
here's a TCB bug.

tions: irrelevant.
oftware: irrelevant.
of lines of code
don't have to check.

eed an audit log? No.
mputers separate? No.
ftware Eve can run? No.

File sharing

So far have described
complete user isolation.

But users want to share
many of their files:
consider the Web, email, etc.

I want to be able
to mark a file I own
as readable to just me;
or also readable to Frank;
or to Eve+Frank;
or to a bigger group;
or to the general public.

Say Fran
makes it

I save a

Later I l

Rememb
Whenev
shows m
it also te
the sour
⇒ Comp
that Fra

I *own* th
but Fran

to check is the
ng base.
1: TCB size.

an's files
CB bug.

levant.
relevant.
f code
e to check.

dit log? No.
eparate? No.
e can run? No.

File sharing

So far have described
complete user isolation.

But users want to share
many of their files:
consider the Web, email, etc.

I want to be able
to mark a file I own
as readable to just me;
or also readable to Frank;
or to Eve+Frank;
or to a bigger group;
or to the general public.

Say Frank creates
makes it readable

I save a copy.

Later I look at the

Remember integrit
Whenever the com
shows me a file,
it also tells me
the source of the f
$\Rightarrow$ Computer has
that Frank was the

I *own* the copy
but Frank is the *s*

is the

ze.

.

No.

No.

No.

File sharing

So far have described
complete user isolation.

But users want to share
many of their files:
consider the Web, email, etc.

I want to be able
to mark a file I own
as readable to just me;
or also readable to Frank;
or to Eve+Frank;
or to a bigger group;
or to the general public.

Say Frank creates a file,
makes it readable to me.

I save a copy.

Later I look at the copy.

Remember integrity policy #
Whenever the computer
shows me a file,
it also tells me
the source of the file.
⇒ Computer has to tell me
that Frank was the source.

I *own* the copy
but Frank is the *source*.

File sharing

So far have described
complete user isolation.

But users want to share
many of their files:
consider the Web, email, etc.

I want to be able
to mark a file I own
as readable to just me;
or also readable to Frank;
or to Eve+Frank;
or to a bigger group;
or to the general public.

Say Frank creates a file,
makes it readable to me.

I save a copy.

Later I look at the copy.

Remember integrity policy #1:
Whenever the computer
shows me a file,
it also tells me
the source of the file.
$\Rightarrow$ Computer has to tell me
that Frank was the source.

I *own* the copy
but Frank is the *source*.

ring

ave described
e user isolation.

rs want to share
their files:
the Web, email, etc.

o be able
a file I own
ble to just me;
eadable to Frank;
e+Frank;
bigger group;
e general public.

Say Frank creates a file,
makes it readable to me.

I save a copy.

Later I look at the copy.

Remember integrity policy #1:
Whenever the computer
shows me a file,
it also tells me
the source of the file.
⇒ Computer has to tell me
that Frank was the source.

I *own* the copy
but Frank is the *source*.

Obvious

The OS
source fo

When m
opens th
the OS
as a sou

When pr
the kern

Typical
don't ev

bed
ation.

share
:
email, etc.

wn
t me;
o Frank;

up;
public.

Say Frank creates a file,
makes it readable to me.

I save a copy.

Later I look at the copy.

Remember integrity policy #1:
Whenever the computer
shows me a file,
it also tells me
the source of the file.
⇒ Computer has to tell me
that Frank was the source.

I *own* the copy
but Frank is the *source*.

Obvious implemen

The OS kernel tra
source for each file

When my copying
opens the file from
the OS kernel mar
as a source for tha

When process crea
the kernel copies s

Typical OS kernels
don't even try to c

Say Frank creates a file,
makes it readable to me.

I save a copy.

Later I look at the copy.

Remember integrity policy #1:
Whenever the computer
shows me a file,
it also tells me
the source of the file.
⇒ Computer has to tell me
that Frank was the source.

I *own* the copy
but Frank is the *source*.

Obvious implementation:

The OS kernel tracks
source for each file, process.

When my copying process
opens the file from Frank,
the OS kernel marks Frank
as a source for that process.

When process creates file,
the kernel copies source.

Typical OS kernels today
don't even try to do this.

Say Frank creates a file,
makes it readable to me.

I save a copy.

Later I look at the copy.

Remember integrity policy #1:
Whenever the computer
shows me a file,
it also tells me
the source of the file.
⇒ Computer has to tell me
that Frank was the source.

I *own* the copy
but Frank is the *source*.

Obvious implementation:

The OS kernel tracks
source for each file, process.

When my copying process
opens the file from Frank,
the OS kernel marks Frank
as a source for that process.

When process creates file,
the kernel copies source.

Typical OS kernels today
don't even try to do this.

nk creates a file,
t readable to me.

copy.

ook at the copy.

per integrity policy #1:
er the computer
ne a file,
ells me
ce of the file.
puter has to tell me
nk was the source.

e copy
nk is the *source*.

Obvious implementation:

The OS kernel tracks
source for each file, process.

When my copying process
opens the file from Frank,
the OS kernel marks Frank
as a source for that process.

When process creates file,
the kernel copies source.

Typical OS kernels today
don't even try to do this.

More co
Eve and
make th

I have a
reads th
reads th
creates a

a file,
to me.

e copy.

ty policy #1:
nputer

file.
to tell me
e source.

ource.

Obvious implementation:

The OS kernel tracks
source for each file, process.

When my copying process
opens the file from Frank,
the OS kernel marks Frank
as a source for that process.

When process creates file,
the kernel copies source.

Typical OS kernels today
don't even try to do this.

More complicated
Eve and Frank cre
make them readab

I have a process th
reads the file from
reads the file from
creates an output

#1:

Obvious implementation:

The OS kernel tracks
source for each file, process.

When my copying process
opens the file from Frank,
the OS kernel marks Frank
as a source for that process.

When process creates file,
the kernel copies source.

Typical OS kernels today
don't even try to do this.

More complicated example:
Eve and Frank create files,
make them readable to me.

I have a process that
reads the file from Eve,
reads the file from Frank,
creates an output file.

Obvious implementation:

The OS kernel tracks
source for each file, process.

When my copying process
opens the file from Frank,
the OS kernel marks Frank
as a source for that process.

When process creates file,
the kernel copies source.

Typical OS kernels today
don't even try to do this.

More complicated example:
Eve and Frank create files,
make them readable to me.

I have a process that
reads the file from Eve,
reads the file from Frank,
creates an output file.

Obvious implementation:

The OS kernel tracks
source for each file, process.

When my copying process
opens the file from Frank,
the OS kernel marks Frank
as a source for that process.

When process creates file,
the kernel copies source.

Typical OS kernels today
don't even try to do this.

More complicated example:
Eve and Frank create files,
make them readable to me.

I have a process that
reads the file from Eve,
reads the file from Frank,
creates an output file.

Integrity policy #1 $\Rightarrow$
The OS kernel marks
both Frank and Eve
as sources for the process,
then sources for the file.

implementation:

kernel tracks
or each file, process.

y copying process
e file from Frank,
kernel marks Frank
rce for that process.

rocess creates file,
el copies source.

OS kernels today
en try to do this.

More complicated example:
Eve and Frank create files,
make them readable to me.

I have a process that
reads the file from Eve,
reads the file from Frank,
creates an output file.

Integrity policy #1 ⇒
The OS kernel marks
both Frank and Eve
as sources for the process,
then sources for the file.

Web bro

Frank po
on his w
My brow
shows it

Integrity
My com
Frank w

A moder
to enforc
But brow
very exp
full of cr

tation:

cks
e, process.

process
n Frank,
ks Frank
at process.

ates file,
source.

s today
do this.

More complicated example:
Eve and Frank create files,
make them readable to me.

I have a process that
reads the file from Eve,
reads the file from Frank,
creates an output file.

Integrity policy #1 ⇒
The OS kernel marks
both Frank and Eve
as sources for the process,
then sources for the file.

Web browsing

Frank posts `news-`
on his web server.
My browser retriev
shows it to me.

Integrity policy #1
My computer tells
Frank was the sou

A modern browser
to enforce this pol
But browser is a m
very expensive to
full of critical bugs

More complicated example:
Eve and Frank create files,
make them readable to me.

I have a process that
reads the file from Eve,
reads the file from Frank,
creates an output file.

Integrity policy #1 ⇒
The OS kernel marks
both Frank and Eve
as sources for the process,
then sources for the file.

Web browsing

Frank posts `news-20140710`
on his web server.
My browser retrieves the file
shows it to me.

Integrity policy #1 ⇒
My computer tells me that
Frank was the source.

A modern browser tries
to enforce this policy.
But browser is a massive TC
very expensive to check,
full of critical bugs.

More complicated example:
Eve and Frank create files,
make them readable to me.

I have a process that
reads the file from Eve,
reads the file from Frank,
creates an output file.

Integrity policy #1 ⇒
The OS kernel marks
both Frank and Eve
as sources for the process,
then sources for the file.

Web browsing

Frank posts `news-20140710`
on his web server.
My browser retrieves the file,
shows it to me.

Integrity policy #1 ⇒
My computer tells me that
Frank was the source.

A modern browser tries
to enforce this policy.
But browser is a massive TCB,
very expensive to check,
full of critical bugs.

mplicated example:
Frank create files,
em readable to me.

process that
e file from Eve,
e file from Frank,
an output file.

policy #1 ⇒
kernel marks
ank and Eve
es for the process,
rces for the file.

Web browsing

Frank posts `news-20140710`
on his web server.
My browser retrieves the file,
shows it to me.

Integrity policy #1 ⇒
My computer tells me that
Frank was the source.

A modern browser tries
to enforce this policy.
But browser is a massive TCB,
very expensive to check,
full of critical bugs.

What if
give Fra
account

Frank lo
stores a
I start a
that loo

If OS tra
then it t
Frank wa

example:
ate files,
ble to me.

hat
Eve,
Frank,
file.

1 ⇒
rks
Eve
process,
he file.

Web browsing

Frank posts `news-20140710`
on his web server.
My browser retrieves the file,
shows it to me.

Integrity policy #1 ⇒
My computer tells me that
Frank was the source.

A modern browser tries
to enforce this policy.
But browser is a massive TCB,
very expensive to check,
full of critical bugs.

What if I instead
give Frank a file-u
account on my co

Frank logs in,
stores a file `news-`
I start a process
that looks at the f

If OS tracks sourc
then it tells me th
Frank was the sou

Web browsing

Frank posts `news-20140710`
on his web server.
My browser retrieves the file,
shows it to me.

Integrity policy #1 ⇒
My computer tells me that
Frank was the source.

A modern browser tries
to enforce this policy.
But browser is a massive TCB,
very expensive to check,
full of critical bugs.

What if I instead
give Frank a file-upload
account on my computer?

Frank logs in,
stores a file `news-20140710`
I start a process
that looks at the file.

If OS tracks sources
then it tells me that
Frank was the source.

Web browsing

Frank posts `news-20140710`
on his web server.
My browser retrieves the file,
shows it to me.

Integrity policy #1 ⇒
My computer tells me that
Frank was the source.

A modern browser tries
to enforce this policy.
But browser is a massive TCB,
very expensive to check,
full of critical bugs.

What if I instead
give Frank a file-upload
account on my computer?

Frank logs in,
stores a file `news-20140710`.
I start a process
that looks at the file.

If OS tracks sources
then it tells me that
Frank was the source.

owsing

osts `news-20140710`
eb server.
wser retrieves the file,
to me.

policy #1 ⇒
puter tells me that
as the source.

rn browser tries
ce this policy.
wser is a massive TCB,
ensive to check,
ritical bugs.

What if I instead
give Frank a file-upload
account on my computer?

Frank logs in,
stores a file `news-20140710`.
I start a process
that looks at the file.

If OS tracks sources
then it tells me that
Frank was the source.

Why sho

Browser
that dow
from Fra

("Creati
—Oh, sh

OS auto
adds UR
for the p

Process
OS tells

-20140710

ves the file,

1 ⇒
me that
rce.

tries
icy.
massive TCB,
check,
s.

What if I instead
give Frank a file-upload
account on my computer?

Frank logs in,
stores a file `news-20140710`.
I start a process
that looks at the file.

If OS tracks sources
then it tells me that
Frank was the source.

Why should this b

Browser creates pr
that downloads `ne`
from Frank's web

("Creating a proce
—Oh, shut up alre

OS automatically
adds URL as a sou
for the process.

Process shows me
OS tells me the U

What if I instead
give Frank a file-upload
account on my computer?

Frank logs in,
stores a file `news-20140710`.
I start a process
that looks at the file.

If OS tracks sources
then it tells me that
Frank was the source.

Why should this be manual?

Browser creates process
that downloads `news-20140`
from Frank's web server.

("Creating a process is slow
—Oh, shut up already.)

OS automatically
adds URL as a source
for the process.

Process shows me the file.
OS tells me the URL.

What if I instead
give Frank a file-upload
account on my computer?

Frank logs in,
stores a file `news-20140710`.
I start a process
that looks at the file.

If OS tracks sources
then it tells me that
Frank was the source.

Why should this be manual?

Browser creates process
that downloads `news-20140710`
from Frank's web server.

("Creating a process is slow."
—Oh, shut up already.)

OS automatically
adds URL as a source
for the process.

Process shows me the file.
OS tells me the URL.

l instead
nk a file-upload
on my computer?

gs in,
file `news-20140710`.
process
ks at the file.

acks sources
ells me that
as the source.

Why should this be manual?

Browser creates process
that downloads `news-20140710`
from Frank's web server.

("Creating a process is slow."
—Oh, shut up already.)

OS automatically
adds URL as a source
for the process.

Process shows me the file.
OS tells me the URL.

Closing

Is the co
even *try*
a softwa
with a s
that enf

If softwa
does thi
security
or does
the com

pload
mputer?

-20140710.

ile.

es
at
rce.

Why should this be manual?

Browser creates process
that downloads `news-20140710`
from Frank's web server.

("Creating a process is slow."
—Oh, shut up already.)

OS automatically
adds URL as a source
for the process.

Process shows me the file.
OS tells me the URL.

Closing thoughts

Is the community
even *trying* to bui
a software system
with a small TCB
that enforces integ

If software security
does this mean th
security is impossi
or does it mean th
the community isn

Why should this be manual?

Browser creates process
that downloads `news-20140710`
from Frank's web server.

("Creating a process is slow."
—Oh, shut up already.)

OS automatically
adds URL as a source
for the process.

Process shows me the file.
OS tells me the URL.

Closing thoughts

Is the community
even *trying* to build
a software system
with a small TCB
that enforces integrity policy

If software security is a failu
does this mean that
security is impossible,
or does it mean that
the community isn't trying?

Why should this be manual?

Browser creates process
that downloads `news-20140710`
from Frank's web server.

("Creating a process is slow."
—Oh, shut up already.)

OS automatically
adds URL as a source
for the process.

Process shows me the file.
OS tells me the URL.

Closing thoughts

Is the community
even *trying* to build
a software system
with a small TCB
that enforces integrity policy #1?

If software security is a failure,
does this mean that
security is impossible,
or does it mean that
the community isn't trying?