RSA Conference 2019

San Francisco | March 4 – 8 | Moscone Center

BETTER.

SESSION ID: BAC -T06

From Ephemeral Infrastructure to Ephemeral Data

Joel Wallenstrom

CEO
Wickr, Inc.
@myWickr

Paul Kocher

Independent

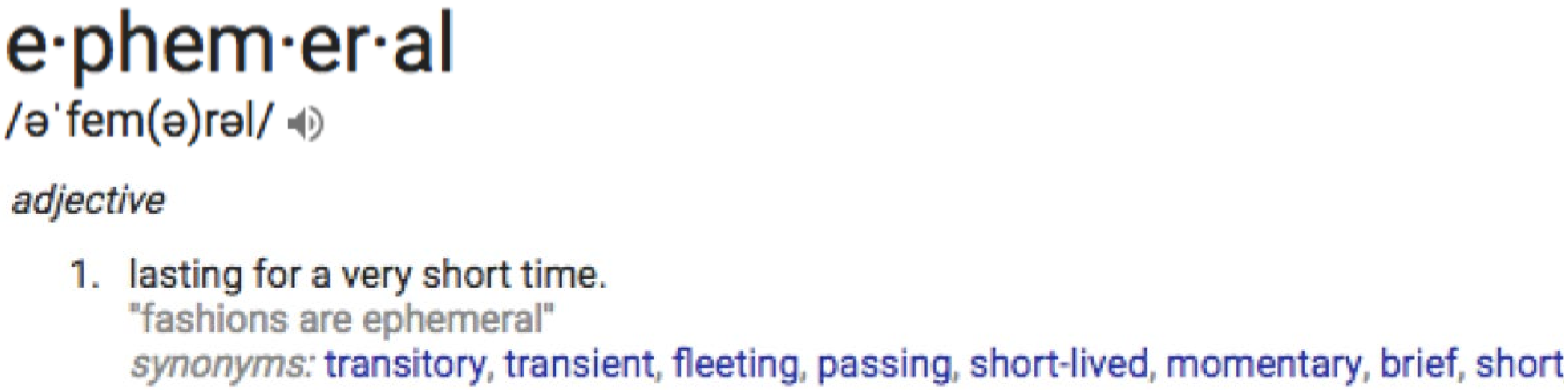
#RSAC

Joel Wallenstrom

- @stake (2000-2004)
  - Acquired by Symantec in 2004
- Founded+ran iSEC Partners (2004-2017)
  - Mobile Security; Red Teaming; Crypto; Research
  - iSEC 100% (ISH) success getting to non-ephemeral data
  - Acquired by NCC Group in 2010
- Investor+CEO Wickr (2014-Present)
  - Open Protocol
  - Transformation from consumer-focused app to secure enterprise collaboration platform trusted by Fortune 500 companies

Paul Kocher

- Founded+ran Cryptography Research (1995-2017)
  - Bootstrapped (no outside investors):
    Consulting → Licensing → Products → Solutions
  - Acquired by Rambus ($342.6M)
- Co-Founded ValiCert (IPO 2001, Acquired 2003)
- Technical projects include:
  - Protocols, incl. co-author of SSL v3 ("🔒")
  - Chip/HW designs (supply chain security, anti-counterfeiting, keysearch…)
  - Timing attacks
  - Differential power analysis + countermeasures
  - Renewability & forensics (Blue-ray BD+…)
  - Factory key management systems (ASICs, devices…)
  - Spectre
- Advisor & investor to many security start-ups
- Member of National Academies' Forum on Cyber Resilience, ACR Fellow, Member of Nat'l Academy of Engineering



e·phem·er·al

/əˈfem(ə)rəl/

adjective

1. lasting for a very short time.
   "fashions are ephemeral"
   synonyms: transitory, transient, fleeting, passing, short-lived, momentary, brief, short

Historical goal: Maximize lifespan of data + infrastructure

Ephemerality: Intentionally limit lifespans

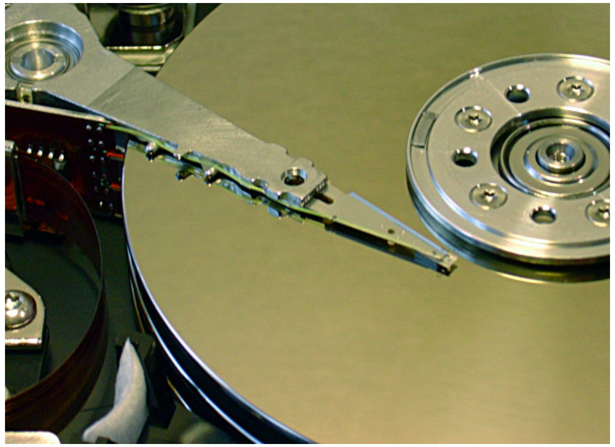
Why minimize persistence?

	Expensive	Dangerous
Persistent infrastructure	Hard to keep running (crashes, outages…) Poor utilization, scaling	Denial of service APTs
Persistent data	Hard to maintain data stores (corruption, synch…) Hard to administer (policies…)	Large masses of data Unbounded attack timeline

Rediscovering ephemeral compute

Compute used to be ephemeral

Lost when internal hard disks arrived



Regaining ephemerality + applying at many layers

amazon web services™ EC2

λ

Microservices

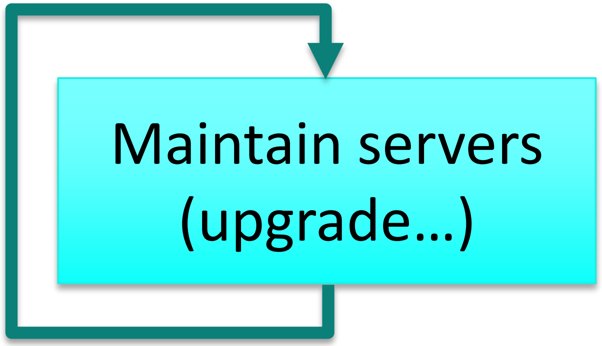
Haskell

SGX

Helps reason about complex systems (facilitate static analysis, reduce development cost, resilience, reduce security risk)

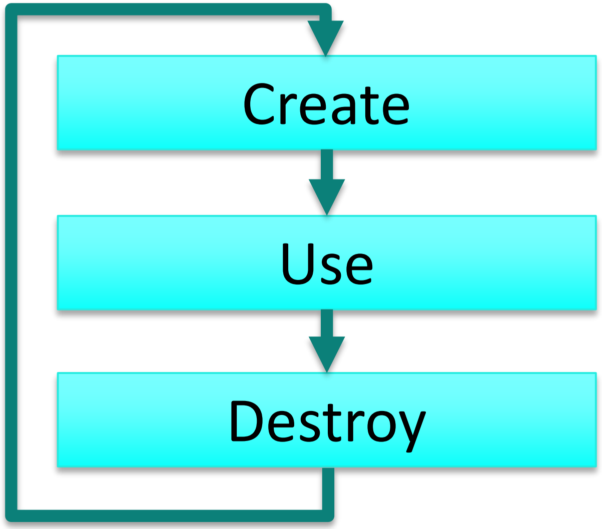
Image of PC by Ruben de Rijcke, CC BY-SA 3.0, https://commons.wikimedia.org/wiki/File:Ibm_pc_5150.jpg
Image of hard drive from user:Petwoe on German Wikipedia, Harddisk-head, CC BY-SA 3.0

Traditional Infrastructure



- Primary focus on maintenance
- Creation is rare
  - Add if capacity < max load
- Destruction is rare
  - Hardware failure/obsolescence

Ephemeral Infrastructure



- Disposable: Creation & destruction are continuous
  - Create when load spikes
  - Destroy when load falls, errors occur, new version…

Ephemerality in Infrastructure: Different way of thinking

- New perspective on architecture
  - Example: Chaos Monkey
    - Kills random instances to ensure server failures don’t impact operation
    - Netflix’s theory: Risks worth subsequent reliability benefits

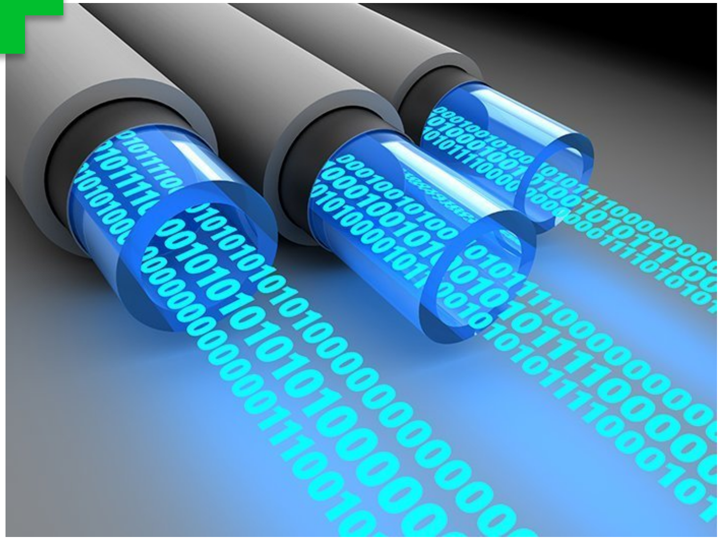


Image of bandwidth_wire https://searchnetworking.techtarget.com/definition/bandwidth
Image of Netflix shows https://www.cordcuttersnews.com

Run Chaos Monkey on Production Systems?!?

Persistent mindset:

The worst possible thing to do!
Systems are mission-critical…
crash one and you'll be fired or arrested

Ephemeral mindset:

Chaos is inevitable
Servers are ephemeral = automate redundancy testing. Better to find & fix problems ASAP

Ephemeral thinking: Chaos Monkey

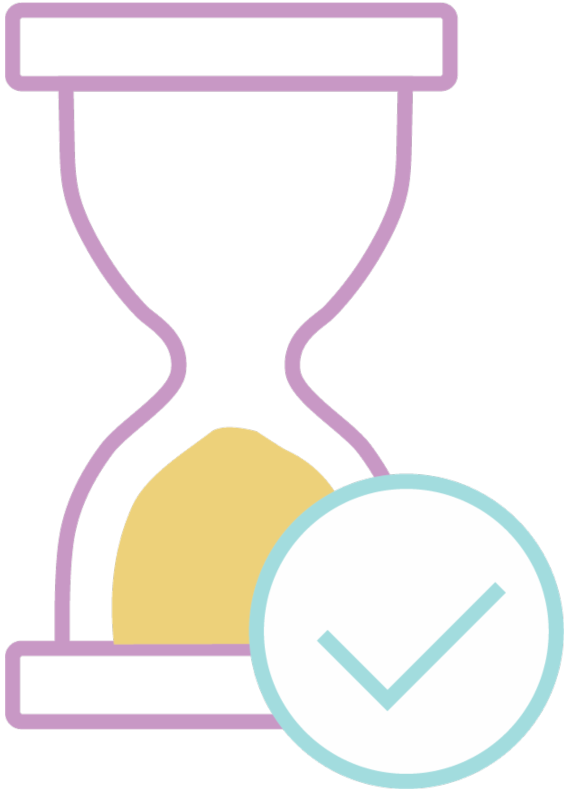
- Chaos Monkey motivation was resiliency
  … but interesting unexpected security benefits

- Lowers value of components to everyone (defenders + attackers)

If attacker…	Consequence
Crashes an instance	Negligible
Corrupts instance data	Less or no impact after instance gone
Exfiltrates instance data	Reduced: instances only has the data it needs (e.g. data for task/customer it's servicing)

Ephemerality in Infrastructure: Different way of thinking

- Ephemeral infrastructure widely used
  - Mature, accepted
  - Elite but going mainstream



What about data?

- Ephemeral data
  - Both ancient and cutting edge

Data Ephemerality is Not New

Data ephemerality is ancient

– Data in transit	Speech, telephone, visible light…
– Data in storage	Archived boxes with “shred by” date

Tech limits: Inability to capture, store

Security: privacy/breach risks, discovery costs

Ephemeral data vs. ephemeral infrastructure

- Challenge for data ephemerality: Data is easily copied
  - Data requires more planning to avoid unmanaged replication

- Huge advantage for data ephemerality: Cryptography

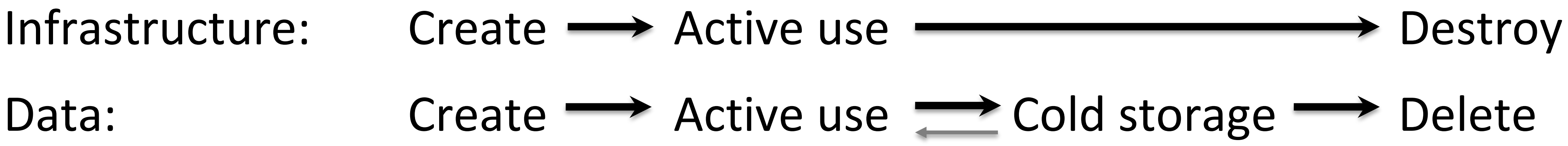
Symmetric cryptography

Simplifies destruction:	Delete key
Simplifies transport:	Encrypt (ephemerality properties of channel don't matter)

Public key cryptography

Simplifies cold storage:	Encrypt with a public key whose private key is offline

Encrypted cold storage: An intermediate stage for data



Infrastructure: Create → Active use → Destroy

Data: Create → Active use ⇄ Cold storage → Delete

- Helps overcome “might want it later” objections
  - Decision #1: Move [X] data into cold storage
  - Decision #2: Delete [X] data
  - But riskier than deletion
    - Partial fix: Define deletion plan when placing into cold storage (e.g. 3 years if not needed)
- Examples:
  - User data not touched recently
  - Log files
  - Backups
  - Regulatory compliance records

Public domain image by Tomwsulcer https://commons.wikimedia.org/wiki/File:Clutter_in_basement.jpg

Cold Storage is Not New

Charles M. Relyea/Library of Congress

Lincoln Hot Letters

Regulatory, legal, business

Retention obligations

- Must keep data until X
- Compatible with hoarding
- Deletion optional afterward (= security benefits)

This requires, in particular, ensuring that the period for which the personal data are stored is limited to a strict minimum.
-- EU GDPR, Recital 39

Deletion obligations

- Must destroy data if X
- Range of potential triggers
  - time (# years)
  - customer asks to be forgotten
  - data no longer useful
  - contract end (NDA expiry)
  - trigger (person dies…)
- Where are all the copies?
  - Backups, logs, employee laptops, persistent servers, databases, crashed hard drives…

Trends & data ephemerality

Technology costs falling exponentially

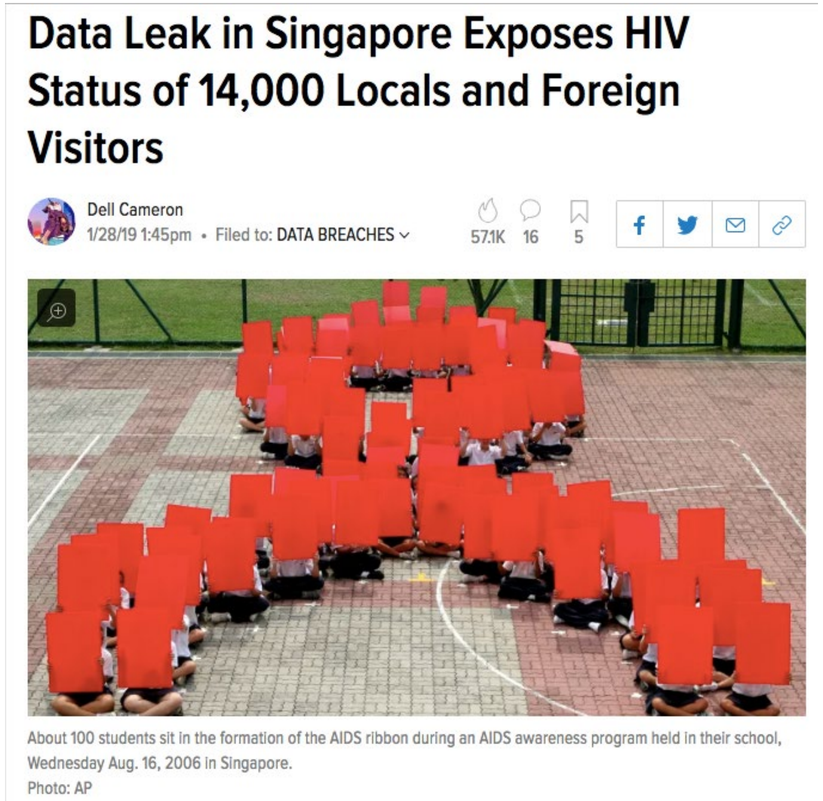
- Storage, collection costs often negligible (for text, audio, images – soon video)

Other costs not falling

- Compliance, legal discovery

Security costs are growing exponentially (but messy)

- Hard to budget: Rare extreme costs, brand risks, regulatory risks
- Hard to allocate: Who control risk != who bears costs
- Hard to quantify: What is a person’s privacy worth?



Data Leak in Singapore Exposes HIV Status of 14,000 Locals and Foreign Visitors

Dell Cameron
1/28/19 1:45pm • Filed to: DATA BREACHES

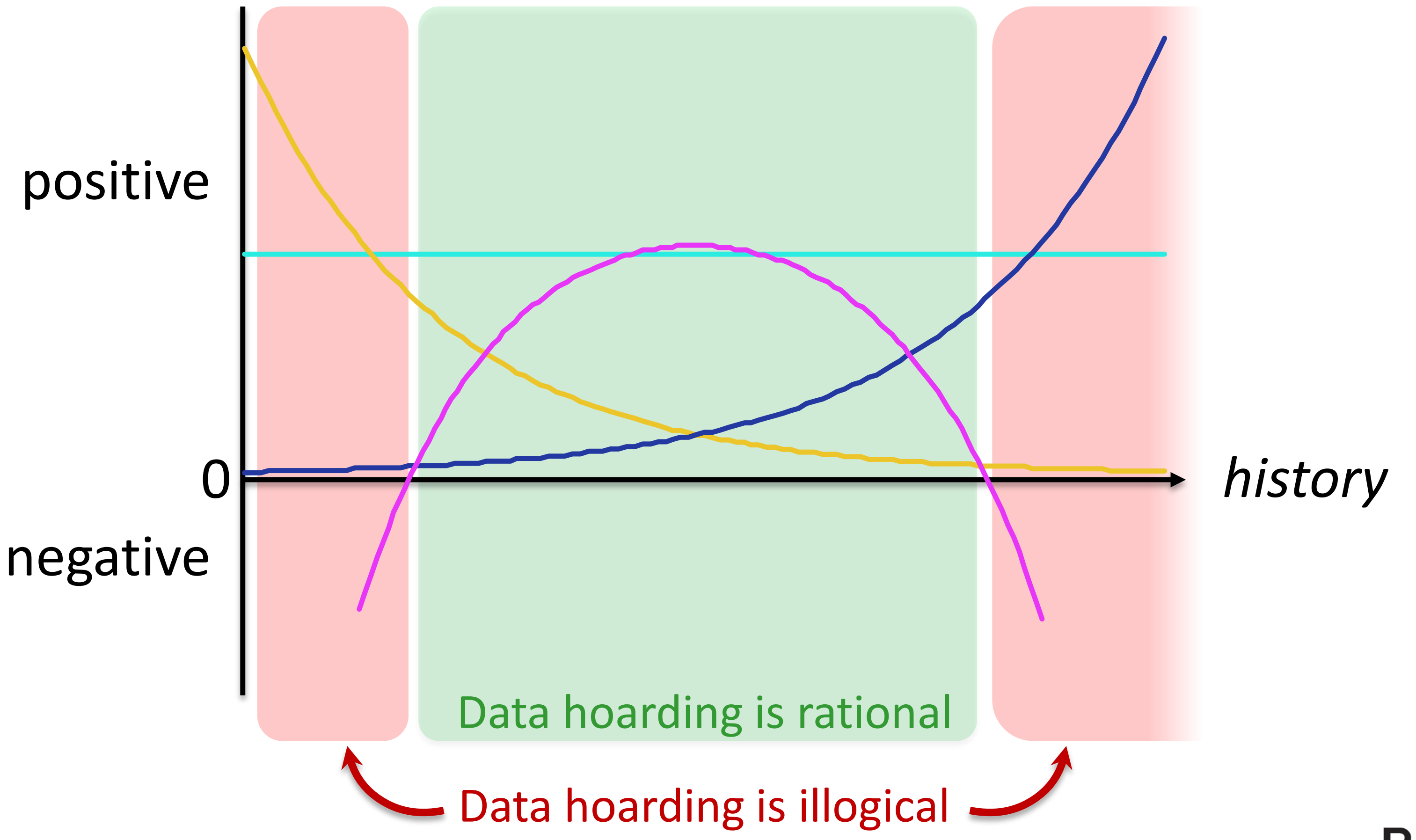
57.1K 16 5

About 100 students sit in the formation of the AIDS ribbon during an AIDS awareness program held in their school, Wednesday Aug. 16, 2006 in Singapore.
Photo: AP

Rational strategies change

(benefit) – (storage cost) – (security cost) = (net value)

Exponential decrease *Exponential increase*



RSA®Conference2019

Apply : Real-world examples of ephemerality

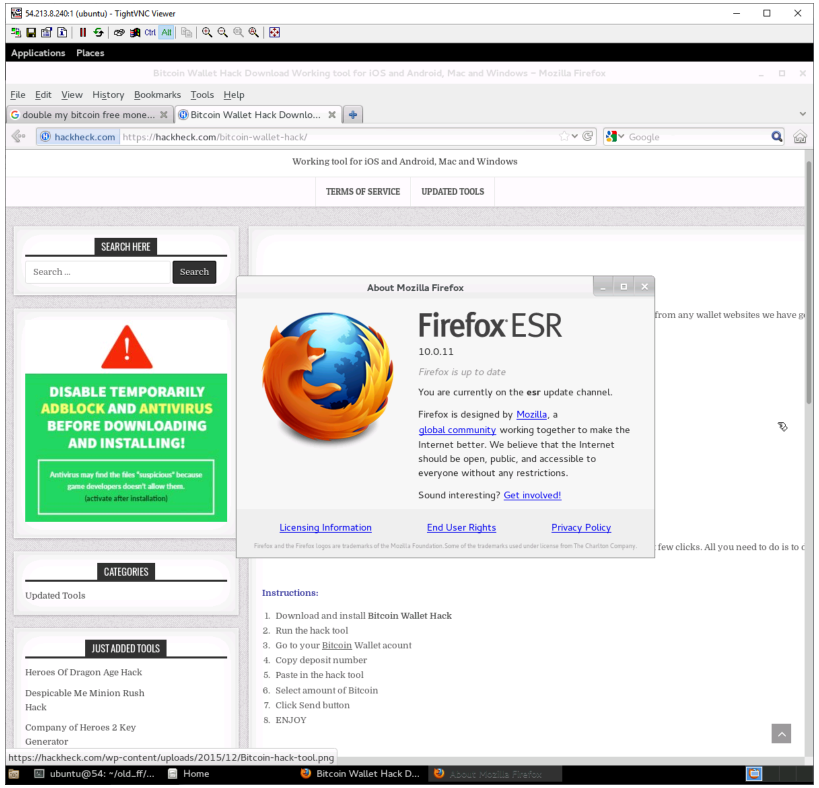
Ephemeral Desktop

- Old model: Developer PCs with local storage
  - ○ Security problem: PCs get lost/stolen, data in/out via USB ports…
  - ○ Cost problem: Most storage & CPU cycles are wasted
- Instead: Diskless thin client
  - ○ Security: Could literally boot from read-only media
  - ○ Cost: Better utilization

Annoying issue: Speed of light

Ephemeral Browsing (aka Browser Isolation)

- Old model: Block 'bad' websites
  - Hopeless: Lists miss bad sites, block sites employees need
  - "Good" sites can still be risky: E.g., Dropbox download, email…
- Ephemeral data + infrastructure:
  - Run browser on a sacrificial instance
  - Browse
  - Kill the instance
- Can create from open source or use commercial offerings


54.213.8.240:1 (ubuntu) - TightVNC Viewer
Ctrl
Alt
Applications
Places
Bitcoin Wallet Hack Download Working tool for iOS and Android, Mac and Windows – Mozilla Firefox
File
Edit
View
History
Bookmarks
Tools
Help
double my bitcoin free mone…
Bitcoin Wallet Hack Downlo…
hackheck.com
https://hackheck.com/bitcoin-wallet-hack/
Google
TERMS OF SERVICE
UPDATED TOOLS
SEARCH HERE
Search …
Search
CATEGORIES
Updated Tools
JUST ADDED TOOLS
Heroes Of Dragon Age Hack
Despicable Me Minion Rush Hack
Company of Heroes 2 Key Generator
About Mozilla Firefox
Firefox ESR
10.0.11
Licensing Information
End User Rights
Privacy Policy
https://hackheck.com/wp-content/uploads/2015/12/Bitcoin-hack-tool.png
ubuntu@54: ~/old_ff/…
Home
Bitcoin Wallet Hack D…
About Mozilla Firefox

Working tool for iOS and Android, Mac and Windows

DISABLE TEMPORARILY ADBLOCK AND ANTIVIRUS BEFORE DOWNLOADING AND INSTALLING!

Antivirus may find the files "suspicious" because game developers doesn't allow them. (activate after installation)

Firefox is up to date

You are currently on the **esr** update channel.

Firefox is designed by Mozilla, a global community working together to make the Internet better. We believe that the Internet should be open, public, and accessible to everyone without any restrictions.

Sound interesting? Get involved!

Firefox and the Firefox logos are trademarks of the Mozilla Foundation. Some of the trademarks used under license from The Charlton Company.

from any wallet websites we have g

few clicks. All you need to do is to c

Instructions:

1. Download and install **Bitcoin Wallet Hack**
2. Run the hack tool
3. Go to your Bitcoin Wallet acount
4. Copy deposit number
5. Paste in the hack tool
6. Select amount of Bitcoin
7. Click Send button
8. ENJOY

- Use an old insecure browser (Firefox v10.0.11)
- Search for "double my bitcoin free money"
- Click on dicey links

Ephemeral Messaging

- Historical model: Unencrypted SMS
  - Message sent as plaintext

Countless trusted entities:

1) Sender, 2) Recipients, 3) Servers, 4) Cloud provider … and … 5) Every node in network

- Typical today:
  - Link encryption between clients and servers
  - Server sees plaintext
  - Archived indefinitely

4 Trusted entities:

1) Sender, 2) Recipients, 3) Servers, 4) Cloud provider

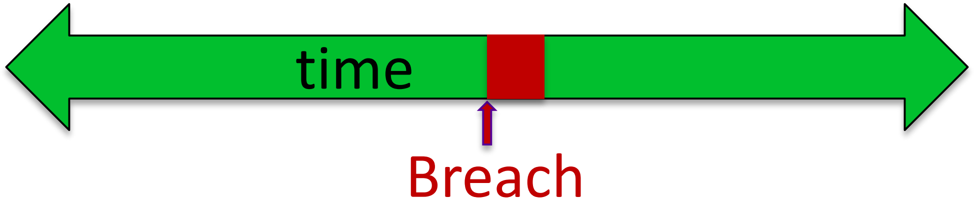
- Ephemeral model:
  - Keys only known to end-points, used once then deleted
  - Deletion models for messages vary
    - Personal: typically automatic deletion with no compliance
    - Business: typically cc a compliance/logging endpoint
  - Deletion mechanism in place before message sent

2-3 Trusted entities:

1) Sender, 2) Recipients; 3) optional compliance/cold storage

Ephemeral Keys

- Forward secrecy & future secrecy
  - Short-lived keys → compromise today doesn't expose past
    - Keys are ephemeral
  - Can combine with future secrecy
    - Key update/ratcheting → compromise doesn't expose sessions occurring after attacker is evicted



- Supported in TLS, some messaging protocols (Signal, WhatsApp, Wickr)

RSA Conference 2019

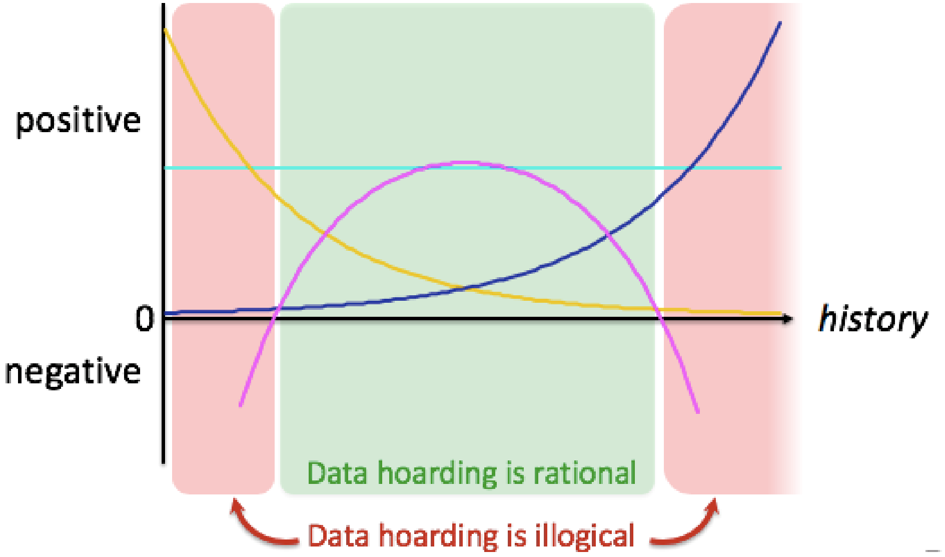
Apply: Making the case

APPLY – Infrastructure Ephemerality

- **Goals**
  - Aim to minimize non-ephemeral infrastructure
  - Won't get to 100% -> benefits don't require 100%
- **Focus**
  - Where can riskiest operations be compartmentalized?
  - Where do compute + storage + network scale differently
- **Analyze**
  - Change in security risk (per node, overall service), +/- cloud vs. tailored
  - Scalability needs
  - Reliability (per node, overall service) & implications of interdependencies in cloud services
  - Re-engineering effort
  - Operational costs at planned scale
- **Architect**
- **Implement**
- **Verify**
  - Chaos monkey…

APPLY – Data Ephemerality

- **Simple Goal.** Begin where data retention is illogical: PII off desktops, sensitive conversations off email…
- **Classify Data.** What data is stored, who is accessing and how often
- **Prioritize Business Needs.** Better classified data helps define data management and analytics processes



- **Update Standards.** Information Governance policies that maximize benefits and minimize risks of data. Ephemerality encourages/forces more explicit, methodical & thorough data life cycle policies
- **Communicate.** Share Information Governance policies in context of business benefits
- **Implement.** Enforce and rely on cold storage. (Storage/Persistence comes with added risk)
- **Orchestrate and Automate.** Use encryption to proactively enforce IG policies