WHAT HAPPENS WHEN COOL IS CREEPY

PRIVACY AND SECURITY WITH BRO - A CASE STUDY

JUNE 20, 2017
INFORMATION SECURITY SYMPOSIUM, UC DAVIS

LISA HO, JOHN IVES, MATT WOLF
UC BERKELEY

[T]he power of new technologies means that there are fewer and fewer technical constraints on **what we *can* do**. That places a special obligation on us to ask tough questions about **what we *should* do**.

- *from President Obama's 2014 speech on NSA surveillance reforms*

WHAT HAPPENS WHEN COOL IS CREEPY

PRIVACY AND SECURITY WITH BRO - A CASE STUDY

Bro
Network
Security
Monitor

Policy on
Privacy and
Online
Monitoring

Policy in Action

BRO COOLNESS

BRO COOLNESS

- Open source, clustered, high-performance network monitoring
  - LBL published a paper on using it at 100G in Aug 2015
- Highly configurable
  - Has its own scripting language
- Not limited to network data
  - Can input logs and analyze them for data and events
- Provides detailed logs of network activity
  - Excellent source for network forensics

BRO

CREEPINESS

BRO

CREEPINESS

A single connection:

1497682767.595403 CScEhf2CC0z0BQoxu1 10.0.0.182 58919
209.188.93.95 80 tcp http 21.684414 [...]

aka Prof. Leading Scholar

Becomes 25 file download events, e.g.,:

1497682768.215956 FduJCE3sefmtxzw0j4 209.188.93.95 10.0.0.182 CScEhf2CC0z0BQoxu1[...] image/png [...]
1497682775.397196 F90zqt2EFyMrsxpt7 209.188.93.95 10.0.0.182 CScEhf2CC0z0BQoxu1[...] text/plain [...]
1497682789.256745 F64uDd10Reu6QHZMH6 209.188.93.95 10.0.0.182 CScEhf2CC0z0BQoxu1[...] text/html [

Which correspond to 25 file http logs, including:

1497682768.004576 CScEhf2CC0z0BQoxu110.0.0.182 58919 209.188.93.95 80 1 GET www.goodtherapy.org /graph/GoodTherapyLogomobile.png http://www.goodtherapy.org/blog/residual-effects-of-childhood-abuse/ [...]
1497682775.327824 CScEhf2CC0z0BQoxu110.0.0.182 58919 209.188.93.95 80 4 GET www.goodtherapy.org /stylesheets/google-font.css http://www.goodtherapy.org/learn-about-therapy/issues/abuse [...]
1497682789.156101 CScEhf2CC0z0BQoxu110.0.0.182 58919 209.188.93.95 80 25 GET www.goodtherapy.org /search-redirect.html?search[zipcode]=94710&search[miles]=25&search[therapist_search]=1 http://www.goodtherapy.org/find-therapist.htm

BRO

CREEPINESS

A single connection:

1497682767.595403 CScEhf2CC0z0BQoxu1 10.0.0.182 58919
209.188.93.95 80 tcp http 21.684414 [...]

aka Prof. Leading Scholar

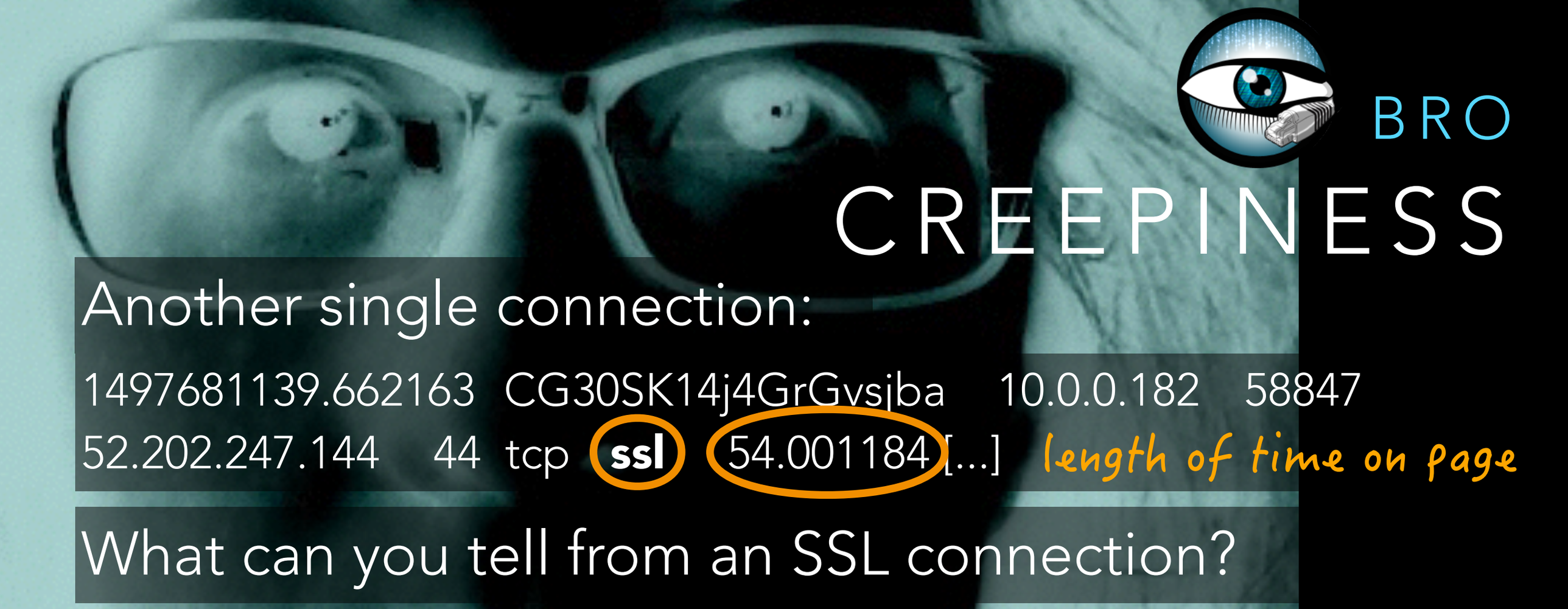
Becomes 25 file download events, e.g.,:

1497682768.215956 FduJCE3sefmtxzw0j4 209.188.93.95 10.0.0.182 CScEhf2CC0z0BQoxu1[...] (empty) image/
1497682775.397196 F90zqt2EFyMrsxpt7 209.188.93.95 10.0.0.182 CScEhf2CC0z0BQoxu1[...] (empty) text/pl
1497682789.256745 F64uDd10Reu6QHZMH6 209.188.93.95 10.0.0.182 CScEhf2CC0z0BQoxu1[...] (empty) t

Which correspond to 25 file http logs, including:

residual-effects-of-childhood-abuse
learn-about-therapy/issues/abuse
search[zipcode]=94710 find-therapist.htm

Not our business



BRO

CREEPINESS

Another single connection:

1497681139.662163 CG30SK14j4GrGvsjba 10.0.0.182 58847
52.202.247.144 44 tcp **ssl** 54.001184 [...] length of time on page

What can you tell from an SSL connection?

- The DNS query for that IP address from dns.log:

1497681139.613890 CBQLqA3UxzvkVWeUA6 10.0.0.182 425688.8.8.8 53 udp [...] www.rainn.org [...] 5

- The browser downloading the SSL certificate from file.log:

1497681139.866227 FUu7tGGl5lqQ2r6fg 52.202.247.14410.0.0.182 CG30SK14j4GrGvsjba SSL [...] application/pkix-cert [...]

And here is the SSL certificate from ssl.log:

1497681139.771164 CG30SK14j4GrGvsjba 10.0.0.182 58847
52.202.247.144 443TLSv12[...] www.rainn.org [...]
CN=*.rainn.org,O=Rape\\, Abuse\\, and Incest National
Network,L=Washington,ST=District of Columbia,C=US [...]

WHAT'S A PRIVACY-CONSCIOUS CAMPUS TO DO?

UC Policies/Reports

ECP
UC ELECTRONIC COMMUNICATIONS POLICY (2000/2005)

UC NON-DISCRIMINATION POLICIES (2013)

PISI
UC PRIVACY AND INFORMATION SECURITY INITIATIVE (2013)

Environmental Drivers

SNOWDEN REVELATIONS (2013)

EXPANSION OF UCB'S INFORMATION SECURITY ONLINE MONITORING PROGRAM

UCB PRIVACY AND ONLINE MONITORING POLICY (2017)

- Transparent review and documented approval of online activity monitoring
- Have a defined process for evaluating privacy impact and balancing privacy values

POLICY ON
PRIVACY AND ONLINE MONITORING

GOALS

- Enable **innovative use of data and technology** in a secure and privacy-respecting manner.
- **Prevent trust-eroding** standoffs over secret surveillance and privacy-invasive monitoring.
- Create a **sustainable framework to manage privacy risks** and articulate why certain practices are acceptable or not.

POLICY ON
PRIVACY AND ONLINE MONITORING

REQUIREMENTS

1. Provide **Meaningful Notice** of monitoring practices

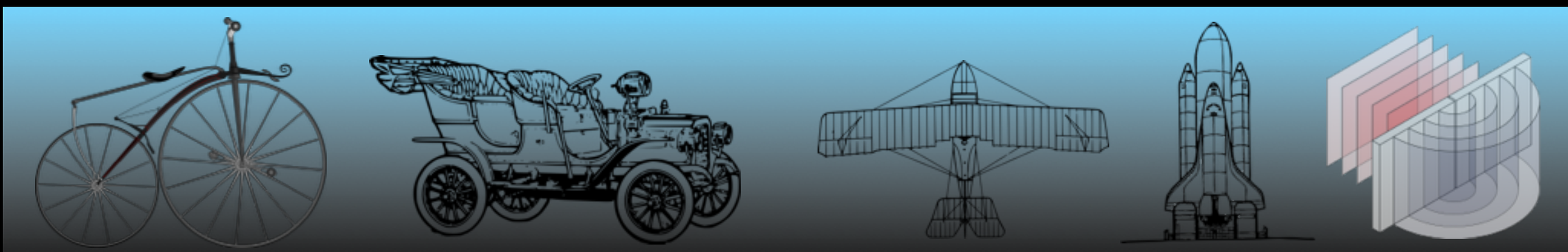
2. Notify governance committees of changes in monitoring practices

3. **If deviating from approved campus norms**:

- Conduct a **Privacy Balancing Analysis**
- **Campus vetting** through **information governance groups**

WHAT'S IN IT FOR SECURITY?

- **Clear decision about permissibility** of a practice -> ***Innovation***
- Requires **clear articulation** of **value** ->
  practice tailored to deliver value
- Helps team **design practices and processes aligned with non-security objectives**
- **Documents approved uses** ->
  policy-based justification **against unapproved uses**
- **Protects information security team from having to decide whether or not to meet external demands for data**



PUTTING POLICY TO WORK: BRO PRIVACY BALANCING ANALYSIS

BRO PRIVACY BALANCING ANALYSIS

UTILITY

Purpose for monitoring and estimate of current and future utility

A. Retroactively and with a very high degree of accuracy, detect malicious sites that were visited prior to the site's inclusion in any threat intel feeds
B. Automate the use of accurate threat intel for suspicious sites and urls
C. Better evaluate the validity of IDS alerts that concern downloaded file
D. Identify phishing sites when a snort/surricata alert is generated from someone insecurely submitting usernames/passwords
E. Determine if users submitted data to phishing sites
F. Better investigate the cause of ransomware and other malware attacks that are frequently the result of drive-by downloads
G. Identify malware downloads using file hashes and threat intel

BRO PRIVACY BALANCING ANALYSIS

ALTERNATIVES

Other means to accomplish the documented purpose, and their relative efficacy and privacy impact

- **Netflow Data:**
  Some of the same value; less adverse privacy impact
- **Enhanced IDS Context:**
  Captures more context around IDS alerts to inform investigation
- **Advanced Endpoint Protection:**
  Mitigates risk of malware from site downloads

BRO PRIVACY BALANCING ANALYSIS

SCOPE

Scope of monitoring, how the utility and privacy impact change if scoped differently

- Option A: Berkeley Campus Network
- Option B: Option A minus residence halls & guest network
- Option C: Critical Assets only

BRO PRIVACY BALANCING ANALYSIS

PRIVACY IMPACT

Data use shall be restricted to documented use cases.

Document the privacy impact and mitigations.

Web browsing data represents the majority of human activity on the internet. Tracking URLs akin to publishing an individual's use of library resources. Reveals private thoughts and evolution of viewpoint in a way that doesn't leave sufficient space for academic freedom.

BRO PRIVACY BALANCING ANALYSIS

USE CASE:

Planned Routine Operational Use

- Automated process to apply threat intelligence feeds (listing compromised IP addresses and malicious URLs, ?, etc..) and identify potentially malicious activity, both as activity occurs and retrospectively as threat intelligence feeds are updated
- Based upon the alerts generated by other IDS solutions that only capture individual packets and do not record packets without a subsequent alert, it will be possible to retrieve the web request that immediately precede the alert. These alerts can be for detected malware as well as signs of users falling for phishing attacks

BRO PRIVACY BALANCING ANALYSIS

USE CASE:

Non-Routine (but Anticipated) Use

- Anticipated occasional uses which may require add'l oversight (short of ECP non-consensual access approval),
- Example scenario: Non-automated investigation of a major security incident
- Example oversight: Notice to Privacy Office, End-of-year accounting to governance committee

BRO PRIVACY BALANCING ANALYSIS

ESCALATION PROCEDURES

Document incident,
obtain approval

- UC Electronic Communications Policy
  - Limitation on circumstances warranting access
  - High-level executive approval requirements

BRO PRIVACY BALANCING ANALYSIS

REQUIRED LEGAL DISCLOSURES

Consider impact of collection and retention of data in case of disclosures required by and consistent with law, e.g., valid subpoena, court order, public records request, national security letter

- While proposed use cases involve only automated review, compulsory disclosures may result in human review
- Bro data may provide insight into private thoughts and ideas that would not be available otherwise
- May be evidence used against UC in litigation

BRO PRIVACY BALANCING ANALYSIS

ADDL BALANCING FACTORS

- Mitigating **Internal abuse** and **Accidental disclosure**
- **Least Perusal**
  - Specify data elements collected
  - Least invasive necessary for stated objectives
  - Automated over manual perusal
- **Least Disclosure** (outside of monitoring unit)
  - Escalation path: generally data subject first, further escalation dependent on urgency
- **Minimal Retention**
- Data **Security**
- **Accountability**: Procedures for ensuring compliance, Reporting/record-keeping, Notice/publication

BRO PRIVACY BALANCING ANALYSIS

PRIVACY EVALUATION / VETTING

- Consider changes to scope/monitoring practice to balance objectives (e.g., anonymize data/separation of duties)
- Bake in Privacy Controls/Safeguards, e.g.,
  - TSA Body Scanners: outline vs body image, viewers locate in separate room away from subject
  - Health Record-style logging/monitoring of access
- Outreach / Campus Comment
- Governance Committee Review
- Iterate

PARTING THOUGHTS

- **Be Transparent**: Engage stakeholders and vet monitoring practices to align with community values
- **Balance**: Apply a structured, policy-based approach to consider privacy impact and resolve conflicting priorities
- **Enable Innovation:** Define process to give structure to evaluate new forms of monitoring
- **Put decisions in the right hands:** Protects custodians of data and data subjects
- **Protect Privacy for the Long Haul**: In a crisis, privacy protections often give way, and over time become eroded. Policy is required to put a thumb on the scale for privacy.

"A society in which people can be monitored at all times is a society that breeds conformity and obedience and submission."

- Glenn Greenwald

QUESTIONS?

IMAGE CREDITS

- Title slide: Ville de Nevers, Drone-007, Lisa Ho
- Outline: bro.org, Eduardo Tavares - Dam Gears, tenor, gears
- Bro Coolness: Dietmar Temps, Glacier Grey, Chile
- Bro Creepiness: Lisa Ho
- Requirements: G B CCK - 'Gunks
- clip art: luc, j4p4n, liftarn, johnny_automatic