Weak keys remain widespread in network devices

Marcella Hastings, Joshua Fried, Nadia Heninger

University of Pennsylvania

Motivation

[Mining Your Ps & Qs: Detection of Widespread Weak Keys in Network Devices: Heninger Durumeric Wustrow Halderman 2012; Public Keys: Lenstra et al. 2012]

- Factored 0.5% of HTTPS RSA public keys on the internet
- Weak keys were due to random number generator failures
- Affected only small network devices
- Major disclosure process to companies producing vulnerable products

What happened? A follow-up study.

- What happened since 2012?
- Did vendors fix their broken implementations?
- Can we observe patching behavior in end users?

Background on Ps and Qs: The GCD Vulnerability

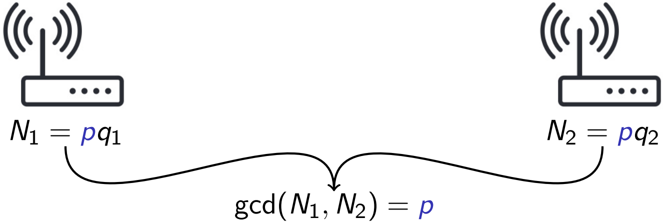
Public Key

$N = pq$ modulus

Private Key

p, q primes

Vulnerability



$\Longrightarrow$ Detect vulnerability by presence of factored key on host.

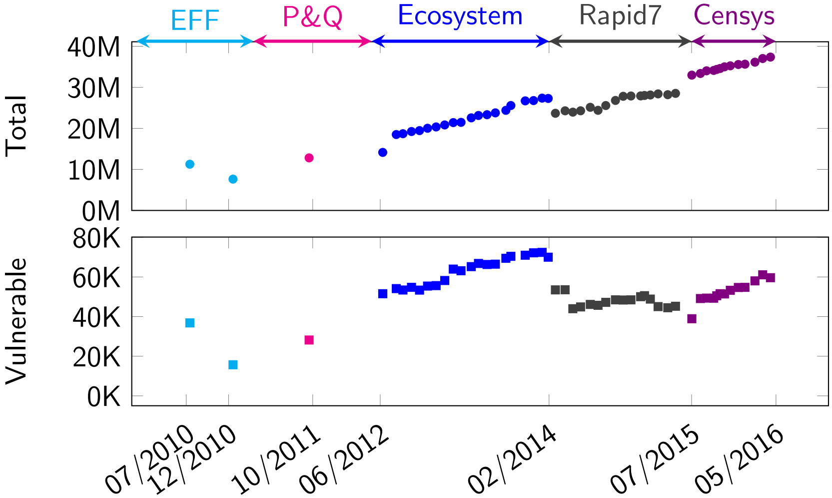
Methodology for this study

What happens when we ask vendors to fix a vulnerability?

1. Aggregated internet-wide TLS scans from 2010-2016
2. Computed GCDs for 81.2 million RSA moduli
3. Identified vendors of vulnerable implementations
4. Examined results based on response to 2012 notification

Data sources: how to read the plots

- Scan sources along top of plot
- Scan dates on x-axis
- Absolute counts on y-axis



Fingerprinting specific implementations

Certificate subjects

- Cisco: `OU=RV120W,O=Cisco Systems, Inc.`
- Juniper: `CN=system generated`
- HP: `O=Hewlett-Packard`
- Xerox: `O=Xerox Corporation`
- Innominate: `O=Innominate`

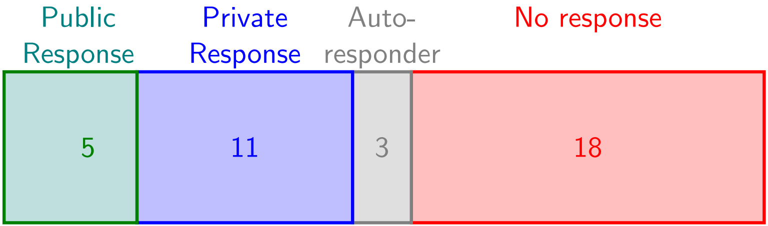
Shared primes heuristic

Shared prime $\Rightarrow$ same implementation.

Original notification

- Low response rates from vendors
- Took place March-June 2012

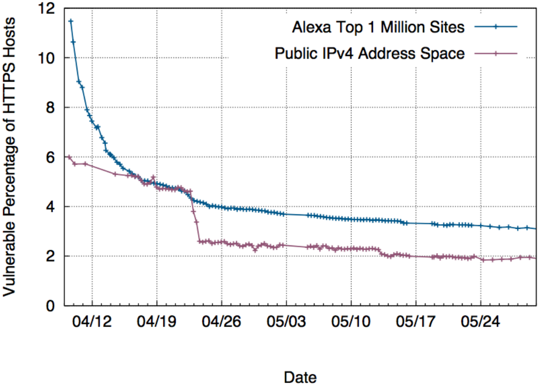
Vendor response to original notification



Research questions: what are we looking for?

Prior work: what we hope to see

- Patch one implementation, notify many users [Debian OpenSSL: Yilek et al. 2009; Heartbleed: Durumeric et al. 2014]



[Durumeric et al. 2014]

Research questions: what are we looking for?

Prior work: what we hope to see

- Patch one implementation, notify many users [Debian OpenSSL: Yilek et al. 2009; Heartbleed: Durumeric et al. 2014]

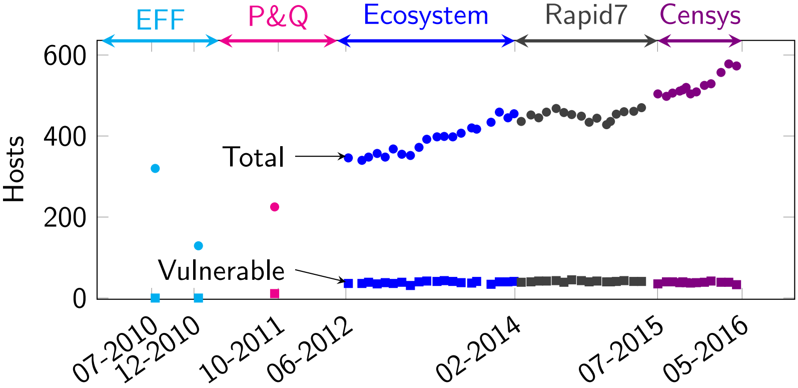
Questions

- What happened with different vendors?
- Did patch rates improve when vendors released a public advisory?
- Do we see the same trends as previous studies?

Innominate

mGuard network security devices (Smart, PCI, Industrial RS, Blade, Delta, EAGLE)

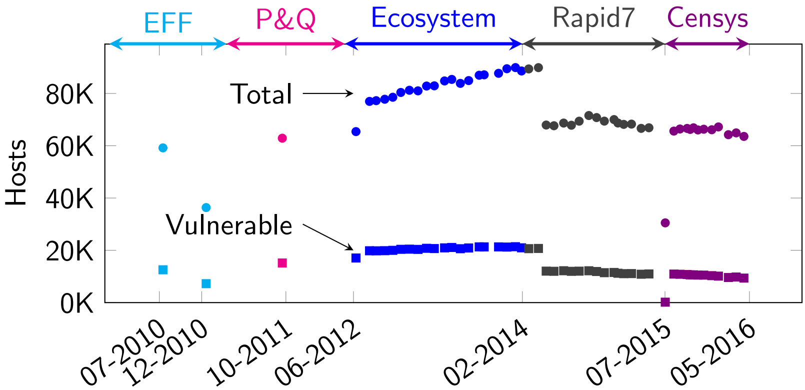
- Public advisory in June 2012
- Consistent population of vulnerable devices since 2012
- New devices not vulnerable, but old devices not patched



Juniper

SRX Series Service Gateways (SRX100, SRX110, SRX210, SRX220, SRX240, SRX550, SRX650), LN1000 Mobile Secure Router

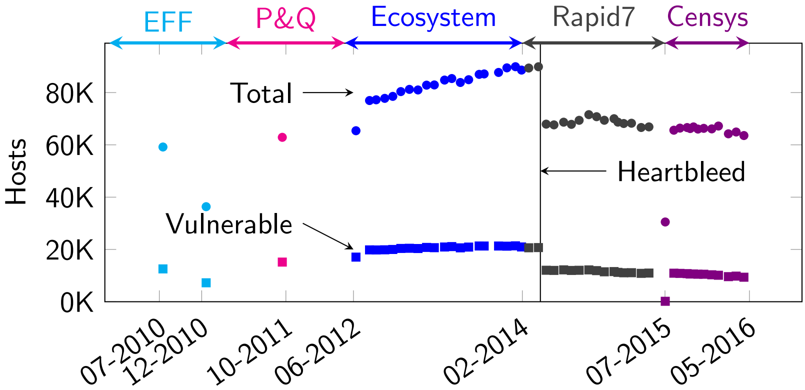
- Public security bulletin in April 2012, out-of-cycle security notice in July 2012
- Majority of factored keys in 2012 were Juniper hosts
- Weird behavior in April 2014



Juniper

SRX Series Service Gateways (SRX100, SRX110, SRX210, SRX220, SRX240, SRX550, SRX650), LN1000 Mobile Secure Router

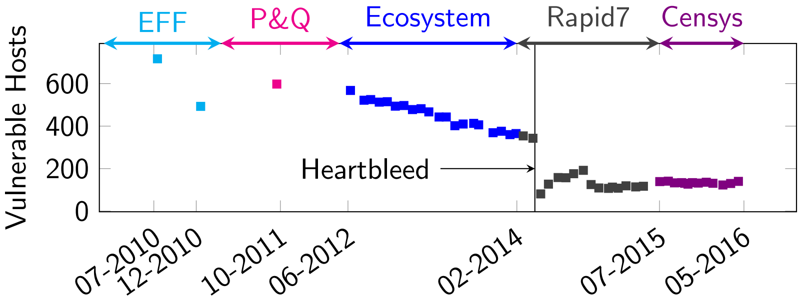
- 30,000 Juniper-fingerprinted hosts (9000 vulnerable) came offline after Heartbleed
- IPs do not reappear in later scans: TLS disabled, scans blocked, devices offline?



IBM

Remote Supervisor Adapter II, BladeCenter Management Module

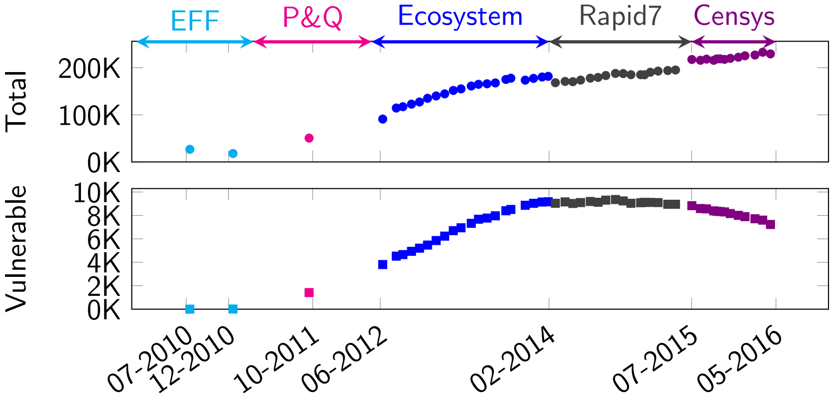
- Public security advisory (CVE-2012-2187) in September 2012
- Prime generation bug: 36 possible public keys from 9 primes
- 100% of fingerprintable moduli are vulnerable



Cisco

RV120W/220W, WRVS4400N, SA520/520W, RVS4000, SA540, RV180/180W, RV130, RV320, RV130W, ISA550/550W, ISA570

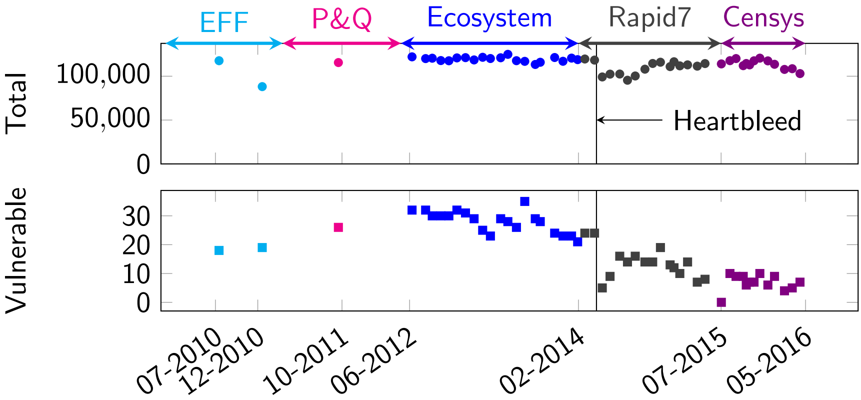
- Substantial private response; no public advisory
- Vulnerable population rises for several years after notification



HP

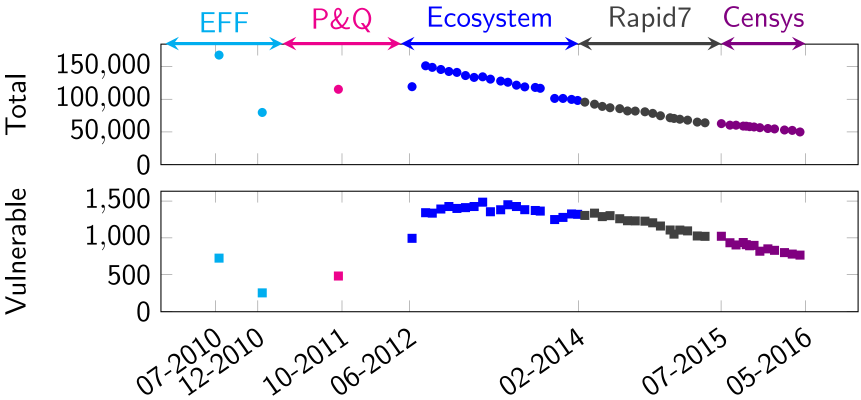
Integrated Lights-Out management card

- Substantial private response; no public advisory
- Internet reports: Integrated Lights-Out (iLO) management cards crash when scanned for Heartbleed



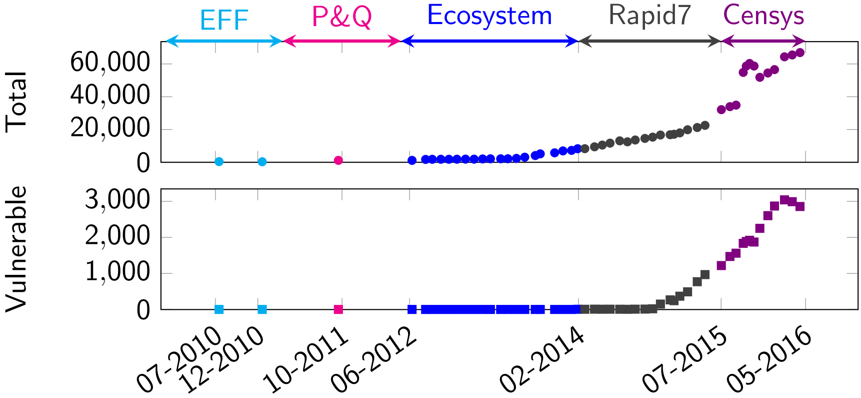
Linksys

- Did not respond to 2012 notification
- No evidence of patching: vulnerability decrease correlated with total decrease



Huawei

- Introduced vulnerability in 2014
- Security advisory published Aug 2016



End-User Patching Behavior

- Few vendors released patches; limited visibility into patching behavior.
- Patching rate is low: Decreasing vulnerability due to device churn.
- Low patch rate for devices has distressing implications for "Internet of Things" security [Yu et al. 2015]
- Vulnerability publicity campaigns (Heartbleed) effective, with unintended consequences

Failure in the Vendor Notification Process

- Security contact information is not available (16/42 vendors had discoverable contacts)
- Few public security advisories
- Organizations such as CERT/CC may increase vendor responses, but don't result in signficant patching behavior [Arora et al. 2010, Li et al. 2016]

Standardizations: RFC 4086

"Care must be taken that enough entropy has been added to the pool to support particular output uses desired."

"Once one has gathered sufficient entropy, it can be used as the seed to produce the required amount of cryptographically strong pseudo-randomness"

Weak keys remain widespread in network devices

Marcella Hastings, Joshua Fried, Nadia Heninger

University of Pennsylvania