POSSE

Portable Open Source Security Elements

Jonathan M. Smith
University of Pennsylvania

http://www.cis.upenn.edu/~posse

Introduction

- PI, Jonathan Smith (Penn)
- Theo de Raadt (OpenBSD project)
- Michael Greenwald (Penn)
- Angelos Keromytis (Columbia University)
- Ben Laurie (AL Group, Ltd.)
- Dale Rahn (Penn)
- Jason Wright (Penn)
- Todd Miller (Penn)
- Stefan Miltchev (Penn)
- Sotiris Ioannidis (Penn)

Background and Motivation

- Security is not about features
- It is about delivering features reliably
- Meeting expectations with no unexpected (and exploitable) behavior
- We have done a very poor job of delivering secure software because we are not willing to expend the "grunt work" (such as audits) that delivering secure software requires
- When traditional software development is used, freeze for audit causes TOAD (Technically Obsolete at Delivery :-)

Consider…

- *"… As an experiment I also planted a comment which should raise eyebrows in some code I released years ago and which is fairly widely used just to see if I'd get any reaction from anyone (the comment says, in effect, "Something really suspicious could happen here", although that's not the real text so you can't just grep for it to find it :-). Noone has ever asked me about this, from which I assume that noone's ever looked at the code they're using. That's kind of scary, because the comment isn't in there just to annoy people, you really could build a rather nasty backdoor in there. There may actually be products out there which are released in binary-only form where the vendor has built in a backdoor at that point, although I saw a posting from* foo@anon.org *in* alt.2600 *saying he'd looked at the product and it was fine, so it must be OK."*
  Peter Gutmann, on PGN's list

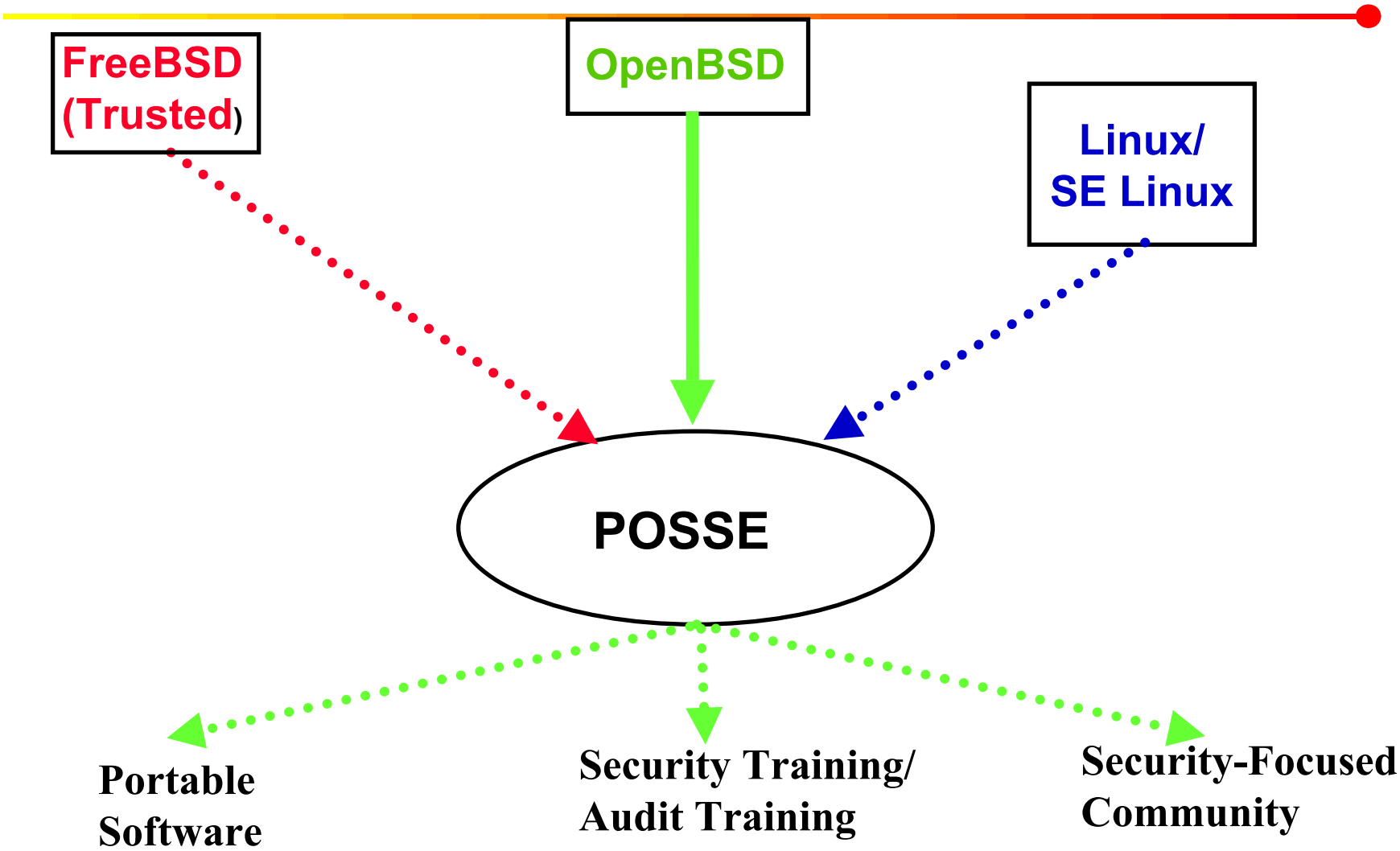
OpenBSD!

- BSD license – most attractive to companies
- Open Source - 4.4 BSD based - split from NetBSD
- Central focus of project is security!
- Led by Theo de Raadt
- No remote root holes in several years
- Development characterized by continuous audit
- Widely used in security products (e.g., IDS) and embedded systems
- See **http://www.openbsd.org**

New Ideas and Approaches (Overview)

- Must keep security in the development mainstream
- Generate a *community* of open source security expertise, by demonstration and code sharing
- Accelerate the introduction of security technologies in both OpenBSD and across *all* open projects; collaborations with TrustedBSD, *etc.*
- Apply OpenBSD audit methodology to OpenSSL
- Document the audit process to disseminate techniques more widely

Model (segue to proposed work)



Proposed Work (short – lots accomplished!)

- 1-liner: "pluck low-hanging fruit"
  - Enable CHATS Phase II
- Social Engineering as much as technology
- Strong genetic ties between BSDs
- Bug fixes in userland propagate w/low (!=0) O.H.
- OpenSSL Audit
  - OpenSSL widely used in e-commerce
  - Part of Apache Web Server (good % of servers)
  - OpenSSL code currently unaudited
  - Opportunity to document methodology => educate!

Proposed Work (details)

- Audit OpenSSL
- Hardware Crypto Support
  - Both symmetric and asymmetric support
  - Important for OpenSSL
- /dev/policy kernel interface for policy rules
  - Prototype policy daemon/kernel done for D.F.
  - Means of importing many SE Linux features
- File system attributes
  - Persistent meta-data for objects (ACLs, labels, caps.)
  - Absorb from TrustedBSD work – R. Watson
- Secure Bootstrap (SEBOS) – W. Arbaugh

Accomplishments - Managerial

- Have hired two people (Dale and Jason) at Penn
- Theo de Raadt (Canadian) under contract
- AL Group, Ltd. (UK) under contract
- Have (thanks to extremely aggressive work by AFRL!) sponsored hackathon previous to Summer USENIX in Boston (June, 2001)
- Sponsored smaller hackathon at USENIX Security
- Audit monograph discussions started w/Ben Laurie (OpenSSL): writing, meld w/technical timelines
- Equipment purchases, provision to TrustedBSD
- To do: Subcontract to Columbia (Keromytis)

Accomplishments – Technical, I

- OpenBSD-inspired changes in OpenSSL crypto framework
- OpenSSL hardware crypto support now working on hifn (Hifn7951) card
- PowerPC support
- RSA smart card support in OpenSSH
- PMTU discovery in IPSEC
- IP stack hardware checksums for some cards
- Fixed DoS problems in passwd and chpass by changing how passwd-file locking is done
- Code-signing effort underway with Ben, Angelos, …

Accomplishments – Technical, II

- Auditing
  - Continue repair of fd_set overflow problems
  - Continue repair of signal handlers
  - Fix syslog() - implementation of syslog_r(), will be re-entrant, also signal safe - addresses signal race problems
  - Incorrect code, e.g., snprintf misuses
- New pf(4) packet filter
  - Replaces ipf (IP problems)
  - Implements some components of "traffic normalization"
  - Address end point traffic interpretation issues e.g., IP fragment or TCP windowoverlays.
  - Can improve some IDS - fewer false alerts

Technical Accomplishments, III

- TCP ISN randomization
  - Proposed in papers (e.g., LBL)
  - First deployment
- Stack offset randomization
  - randomly sized gap is placed at the top of user stack
  - Trouble for fixed size buffer overflow attacks
  - Enabled using sysctl(8)
- RC4 RC4, MD5, SHA1 (not HMAC) in crypto framework (see crypto(9)); DES-CBC, 3DES-CBC, and RC4 work from userland
- Apache policy module (based on KeyNote)

Deliverables and Timeline - POSSE