Lecture 27 – Network Defense 3: Wireless & Other Protocols

Ryan Cunningham
University of Illinois
ECE 422/CS 461 – Fall 2017

Security News

- Mobile Pwn2Own contest concluded
- ONI ransomware attacks in Japan

FINISHING UP NIDS

NIDS Signature Detection

- Application layer reconnaissance/attacks
  - Look for known attack patterns in specific protocols
  - e.g. DHCP, IMAP, IRC, NFS, POP, SMTP, Telnet
  - Find buffer overflow, password guessing, malware transmission
- Transport layer reconnaissance/attacks
  - Look at TCP/UDP traffic to identify known attacks
  - Port scans, packet fragmentation, SYN floods
- Network layer reconnaissance/attacks
  - Look at IP, ICMP for spoofed IP addresses/illegal IP headers

NIDS Signature Detection

- Unexpected application services
  - Look for traffic that indicates an unwanted application
  - IRC/chat clients common for botnets
  - TOR/BitTorrent traffic might not be a good sign
- Policy violations
  - Look for inappropriate website visits
  - Video game/social network use

NIDS Anomaly Detection

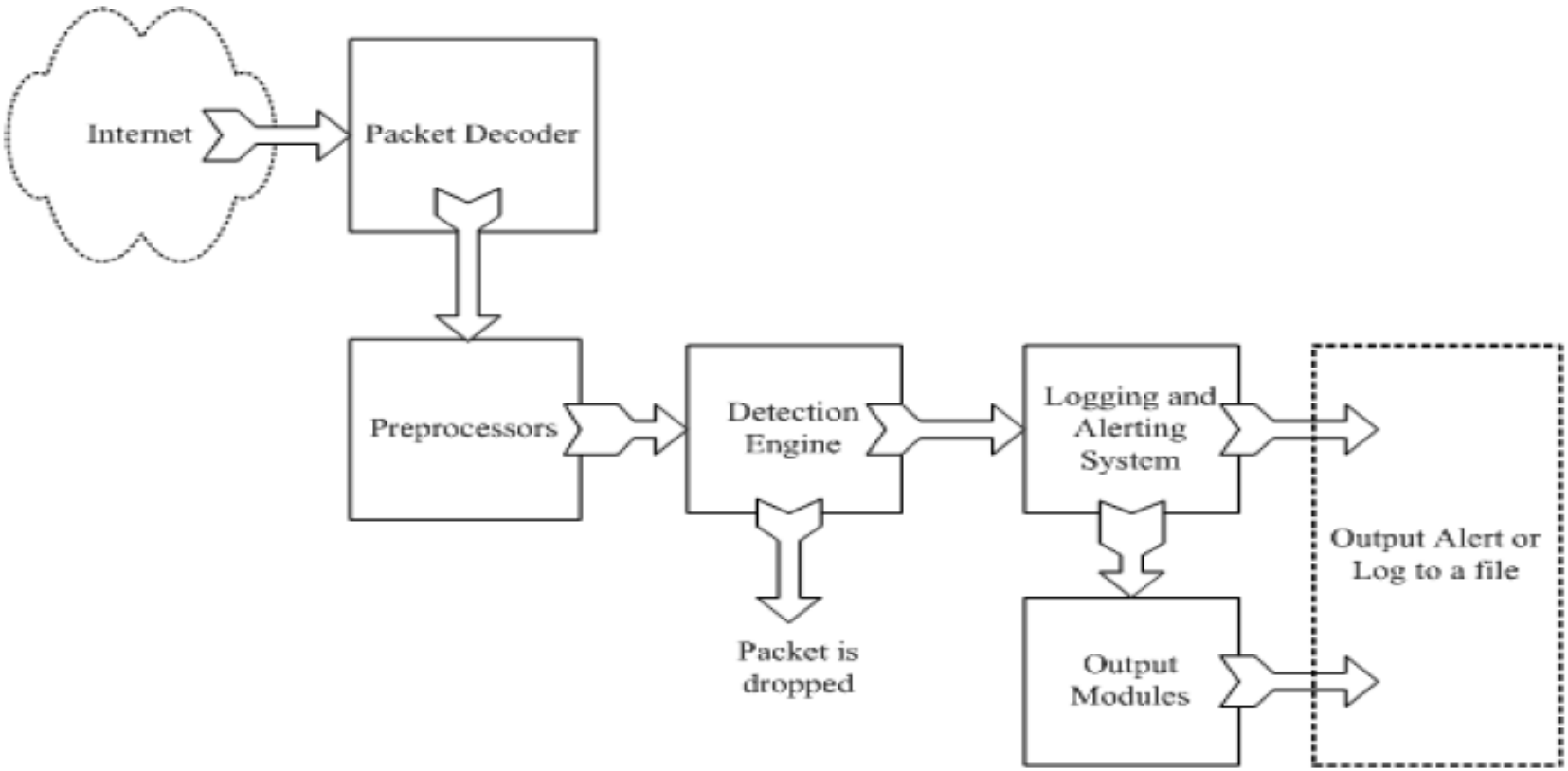
- DoS attacks
  - Look for increased traffic/connection attempts
- Scanning
  - Look for atypical flow patterns at application layer, transport layer, or network layer
- Worms
  - Look for hosts communicating that typically don't
  - Look for ports used that typically arent

NIDS Stateful Protocol Analysis (SPA)

- NIDS can also be used to observe state of connections
- Make sure they proceed as normal
- SPA has a high resource cost

Example: Snort

http://www.snort.org/

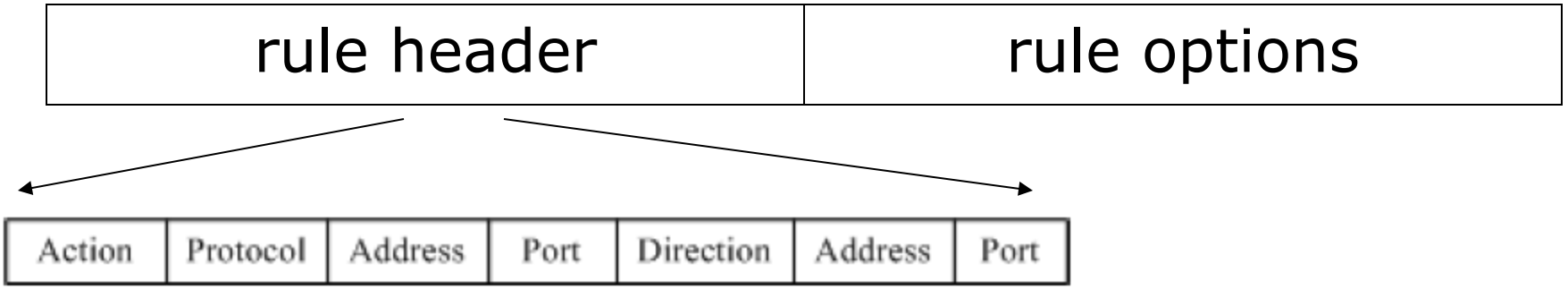


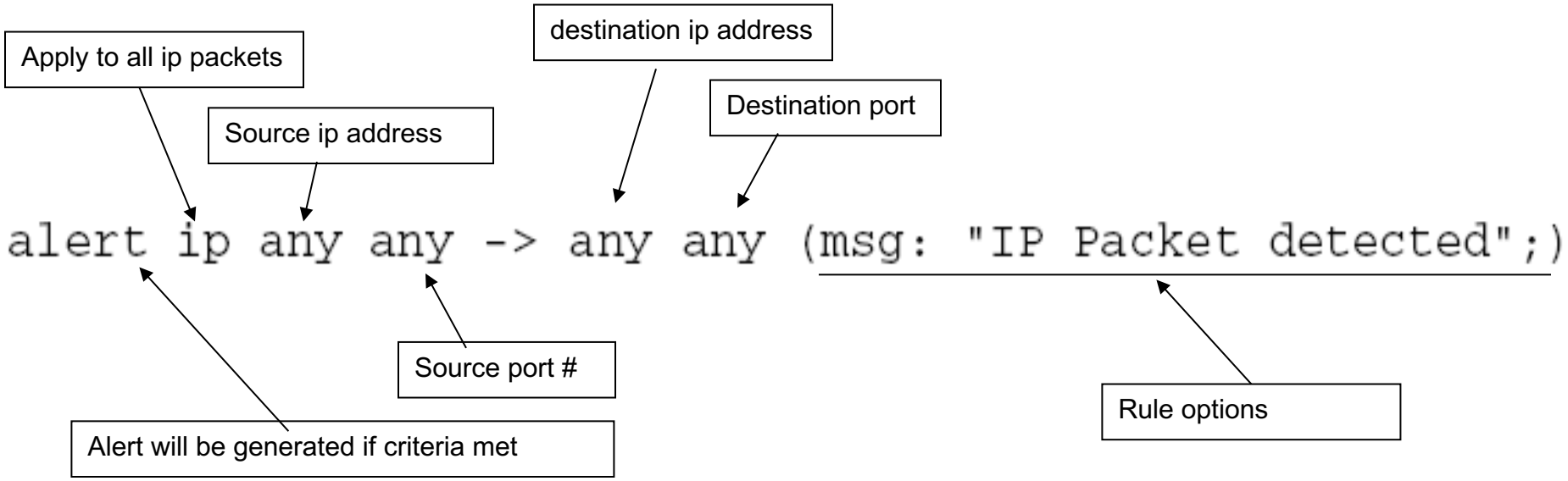
From: Rafeeq Ur Rehman, *Intrusion Detection Systems with Snort: Advanced IDS Techniques with Snort, Apache, MySQL, PHP, and ACID.*

Snort components

- Packet Decoder
  - input from Ethernet, SLIP, PPP…
- Preprocessor:
  - detect anomalies in packet headers
  - packet defragmentation
  - decode HTTP URI
  - reassemble TCP streams
- Detection Engine: applies rules to packets
- Logging and Alerting System
- Output Modules: alerts, log, other output

Snort detection rules





Additional examples

alert tcp any any -> 192.168.1.0/24 111
(content:"|00 01 86 a5|"; msg: "mountd access";)

alert tcp !192.168.1.0/24 any -> 192.168.1.0/24 111
(content: "|00 01 86 a5|"; msg: "external mountd access";)

! = negation operator in address

content - match content in packet

192.168.1.0/24 - addr from 192.168.1.1 to 192.168.1.255

https://www.snort.org/documents/snort-users-manual

Using an IDS

- Plan your incident response process well before you install the system
- Know what you're looking for
- Make the system comprehensive
- Don't overreact to alarms
- If using a rules-based system, keep up with vulnerability reports

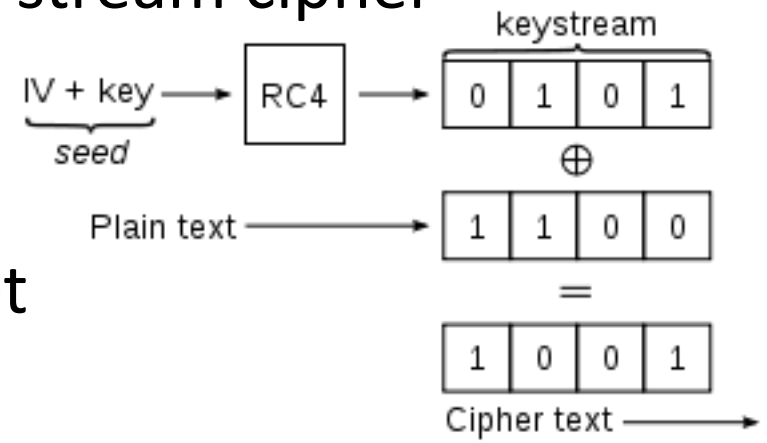
WIRELESS SECURITY

WEP Authentication

1. Host requests authentication from access point
2. Access point sends 128 bit nonce
3. Host encrypts nonce using shared symmetric key
4. Access point decrypts nonce, authenticates host

Wired Equivalent Privacy (WEP)

- Secrecy protected using RC4 stream cipher
- Host and AP share 40-bit symmetric key
- Host appends 24-bit IV to get 64-bit seed
- 64-bit seed used to generate key stream k_iIV
- $c_i = d_i \oplus k_i$IV
- IV and c_i sent to AP for decryption



Breaking WEP encryption

- 24-bit IV, one IV per frame → IV's are reused
- IV transmitted in plaintext → IV reuse detected
- Attack:
- Mallory causes Alice to encrypt known plaintext d_1 d_2 d_3 …
- Mallory sees $c_i = d_i \oplus k_i IV$
- Mallory knows, c_i and d_i She can compute $k_i IV$
- Mallory knows key stream for this IV $k_1 IV$ $k_2 IV$ $k_3 IV$…
- Next time IV is used, Mallory can decrypt

WiFi Protected Access (WPA)

- Initial protocol suite (TKIP) built using WEP components for easy replacement
- Uses unique and stronger keying for each packet, message authentication codes, and crypto hashes
- WPA2 uses AES

Other Secure Protocols

S-BGP Design Overview

- IPsec: secure point-to-point router communication
- Public Key Infrastructure: authorization for all S-BGP entities
- Attestations: digitally-signed authorizations
  - Address: authorization to advertise specified address blocks
  - Route: Validation of UPDATEs based on a new path attribute, using PKI certificates and attestations
- Repositories for distribution of certificates, CRLs, and address attestations
- Tools for ISPs to manage address attestations, process certificates & CRLs, etc.

Slide: Steve Kent

DNSSEC

- Essentially no change to DNS packet format
  - Goal is authentication and integrity, not confidentiality
- New Resource Records (RRs)
  - RRSIG : signature of RR by private zone key
  - DNSKEY : public zone key
  - DS : crypto digest of child zone key
  - NSEC / NSEC3 authenticated denial of existence
- Lookup referral chain (unsigned)
- Origin attestation chain (PKI) (signed)
  - Start at pre-configured trust anchors
    - DS/DNSKEY of zone (should include root)
  - DS → DNSKEY → DS forms a link

IPv6

- IPv6 – new IP protocol with improved security features (IPSec is integrated, discourages fragmentation)

DKIM

- Stands for DomainKeys Identified Email
- Objectives:
  - Prove email actually came from source domain
  - Prevent Phishing/SPAM
  - Verifies path of email
- DKIM proves authenticity of *header only*
- Transparent to end user
  - Implemented by the mail server
  - *Server* signs email (RSA/SHA)

DKIM

CS 461 on Piazza <no-reply@piazza.com> October 3, 2014 3:00 AI

To: Ryan Cunningham <rcunnin2@illinois.edu> Hide Detai

Received: from pps04.cites.illinois.edu (192.17.82.101) by CITESHT3.ad.uillinois.edu (192.17.212.153) with Microsoft SMTP Server (TLS) id 14.3.195.1; Fri 3 Oct 2014 03:00:17 -0500

Received: from o1.sendgrid.piazza.com (o1.sendgrid.piazza.com [75.126.253.244])
by pps04.cites.illinois.edu (8.14.5/8.14.5) with SMTP id s9380HfC020563
(version=TLSv1/SSLv3 cipher=DHE-RSA-AES128-SHA bits=128 verify=NOT)
for <rcunnin2@illinois.edu>; Fri, 3 Oct 2014 03:00:17 -0500

Received: by filter0117p1mdw1.sendgrid.net with SMTP id filter0117p1mdw1.833.542E5785C 2014-10-03 08:00:05.757406501 +0000 UTC

Received: from smtp.sendgrid.net (ec2-107-21-122-172.compute-1.amazonaws.com [107.21.122.172])
by ismtpd-021.iad1.sendgrid.net (SG) with ESMTP id 148d505e1e1.472d.cef712
for <rcunnin2@illinois.edu>; Fri, 03 Oct 2014 08:00:05 +0000 (GMT)

bh=pqcz0Pau84iBTZ81SlZZmhFvWO0=; b=CcAjfLdpd68Ohc1E7A C75eh1FLwbSdsURibOhM/30op3ardsxm0L44bpW4ZVELNYNY5oYzuD/itxe3Hkxt Q5B9HmLSX7fkNJ7+HSbgbwaeiLDZphCE4Cu7SvBlqmpujAlmmGcRh7g7ReA1WDwV Y0WF4/RiGe8Wcx4eKMv5EeSLs=

Domainkey-Signature: a=rsa-sha1; c=nofws; d=piazza.com; h=from:to:references:subject:mime-version:content-type; q=dns; s=smtpapi; b=H97yRuGQ2P/ AhGSXIL78R2z7Rvu2Ild3mS0zgDm5QZ1LJmNvvWc 59xn4pMis9UEGiM+gvmAO176zgxqykhraybTVnd6tHhoC8ZwCHAt0DFxrigzTUov G6Ng/ 7nEZCpJlLtJbWhY54N+rGTBCThiXoHpM146pi4dxrsArwxEU+OU=