CUTLASS - Encrypted Communications for Everyone

Todd MacDermid

CUTLASS Overview

- Started in April, 2004
- Encrypted P2P voice, file, and chat software
- BSD license
- 3 core part-time developers, one full time in May 2005

Questions I Hope To Answer

- What is the target audience?
- Why doesn't existing software work?
- How does it work?
- What have you done so far?
- How can we help?

(This) Talk Rules!

- Questions Whenever

The Dream...

How Much of Your Traffic do **YOU** Encrypt?

The Problem


Safari File Edit View History Bookmarks Window Help
(99%) Wed 5:12 PM
Minnesota court takes dim view of encryption | CNET News.com
http://news.com.com/Minnesota+court+takes+dim+view+of+encryption/2100-1030_3-571
Google
Apple .Mac Amazon eBay Yahoo! News
Minnesota court takes dim ...
CNET tech sites: Product reviews | Shop | Tech news | Downloads | Site map
c|net NEWS.COM TECH NEWS FIRST
E-mail alerts | News.com Extra
FRONT PAGE
ENTERPRISE SOFTWARE
ENTERPRISE HARDWARE
SECURITY
NETWORKING
PERSONAL TECH
THE NET
Track thousands of Web sites in one place: Newsburst
SEARCH
ADVANCED SEARCH
The Net >> Business & legal
Minnesota court takes dim view of encryption
Published: May 24, 2005, 3:02 PM PDT
By Declan McCullagh
Staff Writer, CNET News.com
TalkBack
E-mail
Print
TrackBack
A Minnesota appeals court has ruled that the presence of encryption software on a computer may be viewed as evidence of criminal intent.
Ari David Levie, who was convicted of taking illegal photographs of a nude 9-year-old girl, argued on appeal that the PGP encryption utility on his computer was irrelevant and should not have been admitted as evidence during his trial. PGP stands for Pretty Good Privacy and is sold by PGP Inc. of Palo Alto, Calif.
The HP Compaq Business Notebook nc6120.
With Intel® Centrino™ Mobile Technology.
hp invent
$350 off and FREE shipping.
Featuring HP's exclusive ProtectTools Security Solutions, plus award-winning HP service.
intel inside
centrino
MOBILE TECHNOLOGY
»Save $350 now
» Roll over for more offers
Business & legal resource center
from News.com sponsors
Windows XP Media Center: Start Something Entertaining

The Problem

- Cryptography is not widely used
- Most users are unwilling to sacrifice convenience for security
- It is dangerous to make encryption for experts only

What Traffic Types Are Protected?

- Voice over IP
- File Sharing / File Trading
- Instant Messaging

What Are Existing Solutions?

- Skype
- WASTE
- TOR
- Jabber
- GnomeMeeting and other Free VoIP

Skype

The Good	The Bad
Encrypted, peer-to-peer voice UI was a marvel of simplicity, both in install and use	Licensing terms are onerous Traffic is dependent on central authentication server (CALEA?) Crypto is questionable and closed Only 5-way conference, max.

WASTE

The Good	The Bad
Encrypted, peer-to-peer file transfer Cross-platform Code is broadly available	Licensing issues are fuzzy, at best No way of removing someone from a group Key exchange is painful

Jabber

The Good	The Bad
Open source Strong cryptography available Cross-platform	Cryptography is optional Voice support specs are not specified

GnomeMeeting, Other Free VoIP

The Good	The Bad
Open source Standards-compliant Cross-platform	Cryptography? “Use IPSec”

TOR

The Good	The Bad
Open source Strong cryptography Cross-platform Anonymity in addition to cryptography	Anonymity requires latency Anonymity weak against attackers that can observe both endpoints TCP only, thus unsuitable for voice

CUTLASS Design Goals

- Easy enough to use
- Cross-platform
- Secure by default
- Useful with small network effect
- Extendable (both functionality + paranoia)
- Independent of central servers

CUTLASS Anti-Goals

- Not a strong anonymity system
- Not restricted to existing standard protocols
- Does not require a global namespace

CUTLASS Protocol Design

- Single protocol for all traffic
- UDP-based, with reliable transport layer
- Anyone has server capabilities
- Peers directly connect, minimal traffic through server

Protocol Advantages

- Easy NAT punching
  - No ephemeral ports if we don't want them
  - One hole is sufficient
- Traffic analysis cannot key on packet type

Protocol Disadvantages

- We must reimplement reliable transport
- We won't have access to kernel timers when we reimplement reliable transport

CUTLASS Cryptography

- SSL/TLS - Requires TCP or equivalent
- PGP and S/MIME - Message-based; very inefficient with many packets
- IPsec - Admit it, IPsec sucks
- SRTP - Too strongly tied to RTP to be helpful

Cryptographic Primitives

- RSA-signed Diffie-Hellman exchange
- Ephemeral AES-256 keys in counter mode
- SHA-1 HMAC on each packet
- No replay protection at the crypto layer (but there will be!)

Key Exchange

Initiator / "Client"

Responder / "Server"

----- $nonce_c$, $H(nonce_c , RSA_s)$, RSA_c ----->

<---------- $nonce_s$, $nonce_c$, RSA_s ----------

---------- DH_c , $SIG_c(DH_c)$ ---------->

<---------- DH_s , $SIG_s(DH_s)$ ----------

Cryptographic Protocol Features

- Confidentiality and integrity
- Perfect forward secrecy
- Server responses are optional based on client knowledge of server key
- RSA key authentication, with password-based authentication coming soon

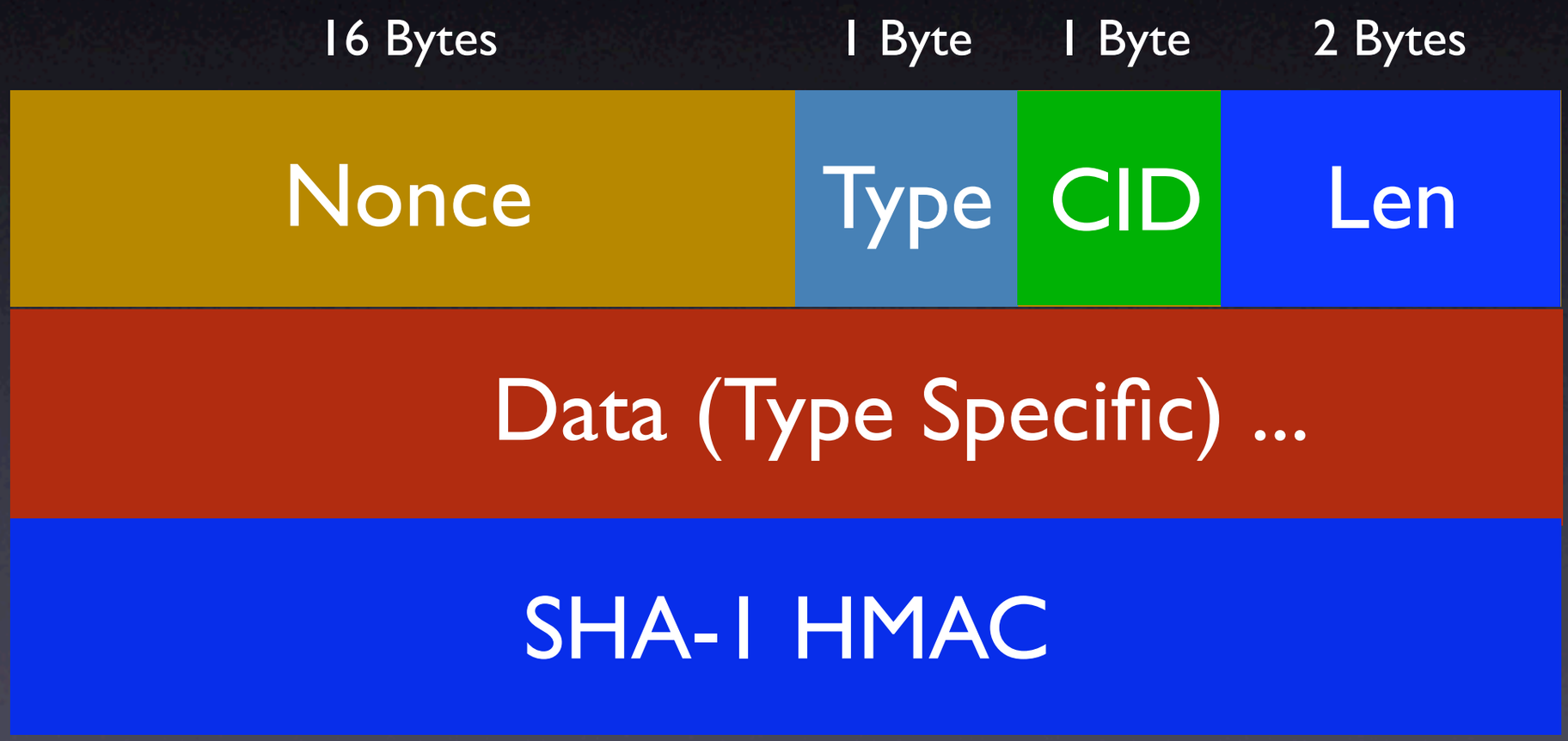
Trust Model

- SSH-style, “Ask on first connect”
- Users primary identification is key fingerprint

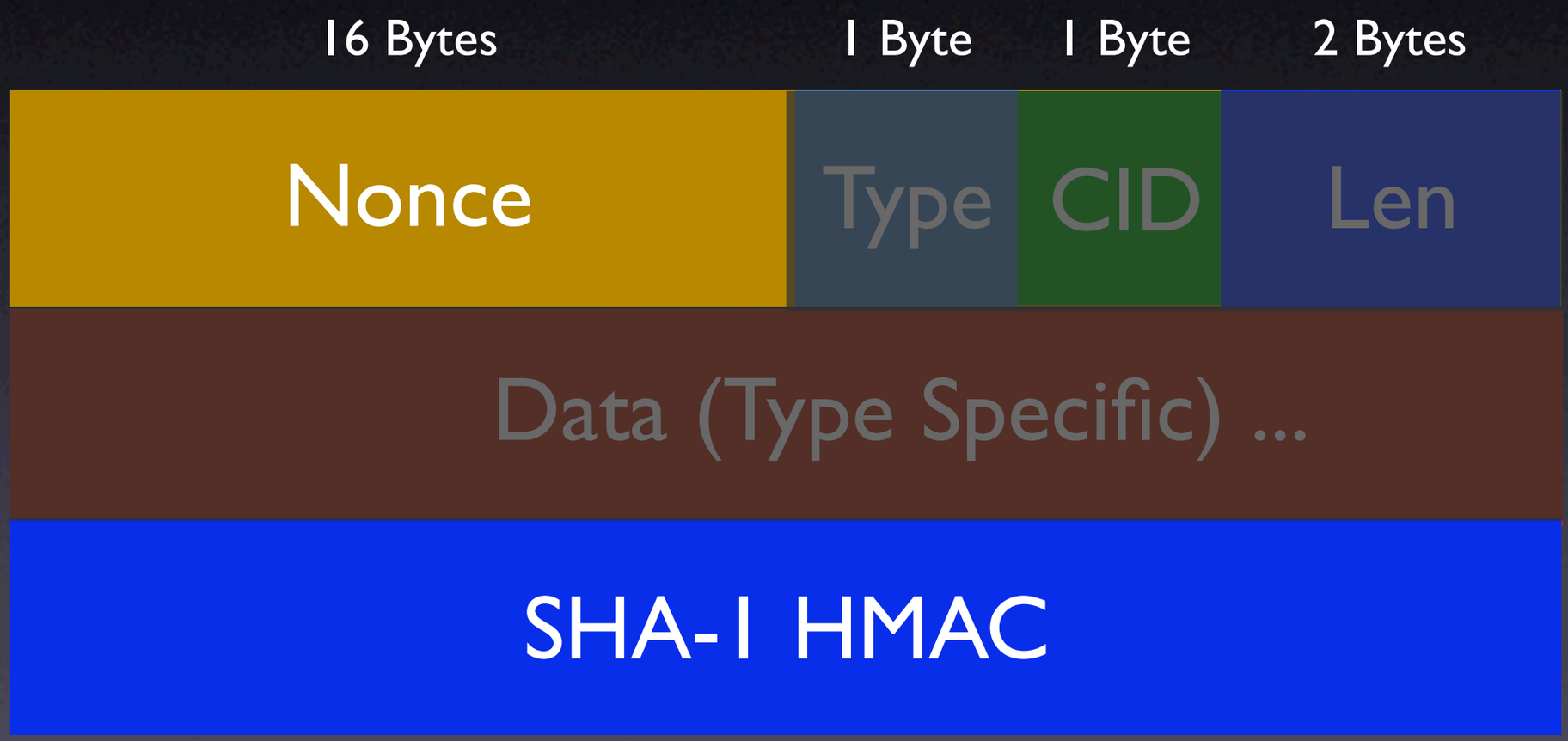
The Five Year Plan

- DTLS - TLS over datagram (IETF draft)
- OpenPGP and SRP authentication for TLS (IETF drafts)
- DTLS + SRP + OpenPGP = sweet

CUTLASS Packet Structure



CUTLASS Packet Encrypted Portions



CUTLASS Packet Types

- Key Exchange
- Ping/Pong
- Connection Information Req/Resp
- Audio
- Reliable Transport

CUTLASS Transport Layer

"Gap"-based requests

0 4500

Request: 0-4500

CUTLASS Transport Layer

"Gap"-based requests

0 4500

Request: 1000-2000,3000-4500

CUTLASS Transport Layer

"Gap"-based requests

0 4500

Request: 3500-4000

CUTLASS Transport Rate-Limiting

- Requests immediately get one response
- Successful request/response pair increases unsolicited rate by one PPS
- Periodically send unsolicited data according to rate
- If number of gaps increases, decrease unsolicited rate

CUTLASS Transport Stats

Copying 34 MB file over 10Mbps local link:

- SCP: 45 seconds
- CUTLASS: 53 seconds

Simultaneous copy bandwidth consumption:

- 75% of bandwidth used by SCP
- 25% of bandwidth used by CUTLASS

CUTLASS Transport Layer Advantages

- Unrestricted by window size
- Easy to turn into Bittorrent-style requests

CUTLASS Voice

- Using Speex, with 8 KHz sample rate
- Phone quality, more or less
- Currently supports OSS
- Anyone willing to write other audio drivers, please join us!

CUTLASS Group Design

- Groups can require authentication or not
- Groups can be advertised on directories
- Group communication is still point-to-point
- Group members are a consensus reality

CUTLASS Group Management

- Ops have a copy of private group key
- Ops cannot be revoked
- Ops may designate lower levels of Op that will not have private key
- These are effectively suggested local policies

CUTLASS Directory Servers

- Anyone can be a directory server
- Store registered users/groups, key fingerprints, and network locations
- Allows searching via strings
- Will NOT store file directories
- Will NOT be initially meshed, but is certainly a future desire

CUTLASS File Servers

- All files requested by hash, not by name
- File names may be searched by strings

What's Done?

- Key Exchange
- Text Messages
- File Push/File Serving
- Directory Serving
- Audio
- GTK Client
- Text Client

LibCUTLASS

- CUTLASS is currently divided into libcutlass and clients
- API docs in tarball
- To use the library, register asynchronous action handlers

Documentation

- action_handler_guide.txt - list of all actions and available information
- api.txt - API usage guide
- internals.txt - thread locking policy and program structure
- protocol.txt - key exchange, cryptography, transport layer, etc

What's Left to Do?

- Group management
- Directory Integration
- Windows, Mac OS X, and PocketPC clients
- Connection forwarding
- Gaim plugin

Cutlass Economic Model

- One full-time developer for 12 months
- Supported by savings, bounties, swag sales, donations
- From there?

Want to Help?

- Join the mailing list
  - cutlass-subscribe@synacklabs.net
- Join in development
  - svn co svn://svn.synacklabs.net/cutlass
- Link the site - http://cutlass.info
- Buy some swag