Week 4 focused on Adam Bates’s NDSS presentation on Wiretapping. The title of this work was *I know They Can Hear You Now*. This work was a survey of past security analysis of the current wiretapping infrastructure and a new addition to improve the wiretapping infrastructure to beat the threats that were found.

There was two parts to the presentation. The first part was the background and the second part was a run through of the NDSS presentation.

**Background**

Adam started by talking about the common standard for wiretapping and how wiretapping works. The law that ensures for a standard wiretapping system is called CALEA. However this is not actually a standard. The standard for wiretapping is called J-Stor (+ a few numbers and dashes).

There are two ways wiretapping worked. The first way (also the old way) is called “loop”. This is where the audio is spliced off the call line and then into the Law Enforcement Agencies (LEA). The second way (and the way it is currently done) splices the audio off to a “delivery function”. If the settings in this function are right (i.e. they want to wiretap one of the two people in the call) then the call goes to the LEA. Once there there is two possible saves.

The first possible wiretap request is also called a “Pen Register”. This is where only the call ”meta-data” is saved. Like who called, the duration, etc. The second kind of a wiretap request is a ”full audio” request. This is the wiretap that everyone thinks of when they think of a wiretap.

There are two types of channels control data channels and content chanel. The control data channel (CDC) has a bandwidth limit of 64kbs. To use either wiretap type an entry must be made using a CDC.

**Vulnerabilities**
There are 5 types of vulnerabilities for wiretapping. (1) Detection of the wiretap. (2) The call data is encrypted (also called obfuscation). (3) Denial of service. (4) Evasion (use the wiretapped line but prevent people from listening in). (5) Confusion (giving false information over a wiretap).

The eavesdroppers dilemma is how much the wiretappee’ (is that a word?) wants to evade vs confuse the LEA.

For a loop network there were two kinds of attacks. (1) Dial spoofing which allows for only one (either the LEA or your friend) from hearing you. (2) C-tone of death which, when a C-tone is played in the background, makes the LEA think the phone is on the hook. A form of the second attack is the "hot pants call" which is when after a "normal" conversation takes place a C-tone is played and then continue to talk after the LEA stop recording.

There are three types of attacks on CALEA systems. (1) a UDP like flood to the control data channel. (2) send packets with bad timestamps to prevent it from being used in court (since a wiretap order also has a valid date range). (3) send packets with false senders or receivers.

And lastly, you can buy wiretapping equipment off ebay!!!! (but don’t cause its Illegal so don’t do it).

NDSS

Ex-Gov Blagojevich’s trial had problems since no one knew if the feds had "minimized" (i.e. removed) data that would vindicate him. This could have been solved if there was a way to verify (audit) the wiretap data.

In 2004 someone wiretapped (illegally) political figures in greece during the olympics. They were never caught. It would be nice if it was possible to detect if wiretaps were happening in the logs that maybe should not have happened. (Since there is not one now).

The main contribution is the "encryptor" which allows for the auditing of logs and prevents a court from using other courts wiretap data.

Then Adam talked a lot about CALEA, J-standard, its archetecture, the way the delivery function works, the bottleneck of the CDC, and if the CDC is resource exhausted then neither wiretap can happen.

There is a 1968 wiretap law which makes audit data availble for the public.

Also another repeat information on injecting bad packets.

New things! The Encryptor. It securely encrypts wiretap data for a log which can be used for (1) to audit and (2) access only the single court’s wiretaps and not all the wiretaps. Central storage is bad, but since that is the way it is done anyways this should not be a new problem.

The threat model includes: Wiretap targets, Unauthorized wiretappers, dishost log maintainers. And the encryptor deals with all of these problems!
Event logging-wise, the even log records (1) the wiretap event (encrypted under the record key), (2) the event count (record key), (3) hard of (1) and (2) (record key), (4) aggregate block (encrypted under the public key of the accountant), and (5) the event timestamp (cleartext).

Courts can audit which returns all records. The court can only successfully decrypt the wiretaps which are encrypted under their own key. Event counter will identify gaps. Accountants can audit by using an additive homomorphic scheme. The private key is then used to decrypt the logs. A party cannot remove records undetected since the sequence numbers will be altered.

There are four types of wiretap messages. Wiretap event, Wiretap start and stop, heartbeat message, and noice. Each one of these four types has a purpose. The first one is for the actual data, the second is for the log counters, and the last two are to prevent (in order) log omissions and timing analysis attacks.

Security analysis: it will detect DOS since all the events will be logged. It will detect unauthorized wiretaps by the sequence data, and it will handle malicious loggers since the log data is encrypted.

This was implemented in Asterisk. It is possible to have 10,000,000 max records in the "encryptor" at one time. Can handle 18,000 calls at the same time (500+ calls for a university at peak time). Could have handled .87% of AT&T’s 2003 traffic and probably up to 10% if optimized. It would take 3 PC’s to log all the data in 2008.

Conclusion

This system thwarts attackers.

Questions

1. What about cell phone data. 2. link-ability 3. how does this handle the athens affair, 4. homomorphic encryption.