Benutzerorientierte Sicherheitskonzepte

Seminar Smart Environments SS 2004

Betreuer Harald Vogt

René Gallati
rgallati@student.ethz.ch

22. Juni 2004

Zusammenfassung

Die Anzahl kleiner, mobiler Geräte, die sich mit ihrer Umgebung vernetzen und Verbindungen mit anderen Geräten in der Nähe aufbauen, wächst stark. Gleichzeitig möchte man von möglichst überall auf seine Daten oder das Internet zugreifen können, sowie elektronisch bereitgestellte Dienste und Services in Anspruch nehmen, gemäss der "Information at your Fingertips" Idee.

Da die beteiligten Geräte, insbesondere die dem jeweiligen Benutzer gehörenden Systeme wie PDAs, Mobiltelefone und Laptops typischerweise dauernd den Standort wechseln, werden in solchen Umgebungen primär kabellose Technologien [1] eingesetzt. Diese auf Funk basierenden Technologien haben aber den Nachteil, dass die Daten für einen Angreifer sehr einfach abhör- und manipulierbar sind.

In dieser Arbeit geht es darum, welche Auswirkungen dies auf die Sicherheit hat und wie man die daraus entstehenden Probleme lösen kann. Dazu werden Lösungsansätze basierend auf ortsbasierter Authentifizierung vorgestellt, welche nicht nur verhindern, dass ein Angreifer unerlaubt Dienste in Anspruch nehmen kann, sondern zusätzlich keine umständlichen Hürden für einen regulären Nutzer darstellen, also möglichst intuitiv zu verwenden sind. Dazu zählt auch die „Drag and Drop“ Interaktion, welche am Schluss als sehr intuitive und einfach zu verwendende Methode behandelt wird.

Inhaltsverzeichnis

1. Einführung

1.1 Das Problem

Wir leben in einer Welt die sich immer stärker vernetzt. Etwas mehr als jeder zweite Westeuropäer besitzt ein Mobiltelefon [2], PDAs verdrängen die papiergebundenen Organiser und Laptops zeigen sich weiterhin wachsender Beliebtheit, genauso wie es auch immer mehr Internetbenutzer gibt. Es ist daher zu erwarten, dass sich die Anzahl der elektronischen Geräte, welche eine Person mit sich herum trägt, insbesondere wenn man das momentan noch reine Forschungsgebiet des „Wearable Computings“ miteinbezieht [3], noch weiter stark steigen wird. Gleichzeitig wird aber auch die Umgebung immer mehr von elektronischen Systemen bevölkert werden – Sensoren welche Warnungen und Hinweise, wie zum Beispiel Baustellen oder Stauwarnungen auf der Autobahn mitteilen werden.
Da aber insbesondere die Klein- und Kleinstcomputer wegen ihres Energiebedarfs und beschränkten Grösse auch auf absehbarer Zeit im Vergleich zu normalen Arbeitsplatz PCs nur limitierte Funktionen und Speicher bieten werden, müssen diese sich mit anderen Systemen vernetzen, um erweiterte Funktionen und Dienste anbieten zu können. Diese Vernetzung kann aber aufgrund der Mobilität und Grösse der beteiligten Geräte zwangsweise nicht drahtgebunden sein. Zum Einsatz kommen daher ausschliesslich WLAN-Technologien, also drahtlose Übermittlungstechniken wie Funk, Infrarot und Infraschall.
Der Vorteil der WLAN Technologien, die relativ einfache Abdeckung eines Gebietes ist aber gleichzeitig ein Nachteil, da ein Angreifer sehr einfach Zugang zum Netz bekommt, unter Ausnutzung von sehr sensitiven Antennen auch aus Distanzen welche enorm grösser sein können als der beabsichtigte Bereich des zur Verfügung gestellten Dienstes. Damit erhöht sich automatisch der Bereich, in welchem Angriffe wie die Man-in-the-middle Attacke (MITM) oder einfaches Abhören nicht verschlüsselter, vertraulicher Informationen möglich sind.
Eine effektive Möglichkeit, den Zugang auf den eigentlich vorgesehenen Bereich einzuschränken bieten ortsbasierte Authentisierungsverfahren an, welche durch technische Methoden sicherstellen, dass ein potentieller Benutzer von Diensten respektive sein Gerät sich auch wirklich im vorbestimmten Bereich aufhält.

1.2 Beispiel MITM Angriff

Bei einem Man-in-the-Middle (MITM) Angriff versucht sich der Angreifer in die Mitte zwischen zwei kommunizierenden Parteien zu schleusen um sich der jeweiligen Seite als Gegenüber auszugeben.

Illustration 1 MITM Angriff

Durch diese Art einer Attacke können auch Public Key Systeme wie sie unter anderem heute zur Sicherung der Kommunikation verwendet werden, erfolgreich unterwandert werden [4]. Solche Angriffe können problemlos detektiert und von vornherein verhindert werden, wenn sich die beiden kommunizierenden Parteien von einer früheren Kommunikation schon kennen und bereits eine

(kryptografisch gesicherte) Vertrauensbeziehung aufgebaut haben. Leider nützt dies aber gerade in einer hochmobilen Welt nichts, wo es in der Regel keine à-priori Trust-Beziehung zwischen den beteiligten Parteien gibt, daher ist diese Art von Angriff durchaus eine ernst zu nehmende Bedrohung.

2. Anforderungen

Einige der wichtigsten Anforderungen an ubiquitäre Netze können wir wie folgt definieren [5]:

- Einfach und Intuitiv
- Sicher
- Fälschungssicher
- Diebstahlsicher
- MITM-sicher

2.1 Einfach und Intuitiv

Ein zu verwendendes System muss einfach sein, da es sonst von einer technisch nicht versierten Mehrheit kaum akzeptiert werden wird oder die zu komplizierten Sicherheitsmechanismen durch die Benutzer abgeschwächt, umgangen oder vermieden werden, indem Passwörter aufgeschrieben, Karten/Tokens anderen Personen ausgeliehen oder ganz einfach der geschützte Dienst nicht in Anspruch genommen wird.

2.2 Sicher

Das System sollte sicher sein, so dass selbst unter den in Punkt 1 aufgeführten Bedingungen ein Angreifer mit *limitierten* Ressourcen nicht einfach an vertrauliche Daten und Rechte gelangen kann.

2.3 Fälschungssicher

Ein vom System akzeptiertes Sicherheitstoken darf nicht von einer nicht autorisierten Person erzeugbar sein. Das Zugangstoken muss also genügend komplex sein, so dass ein Angreifer, der ein gültiges Token sieht, sich selber keine Kopie oder ein ähnliches, ebenfalls akzeptiertes Token konstruieren kann.

2.4 Diebstahlsicher

In der Welt der mobilen und kleinen Geräte ist es leicht, ein Gerät oder Token unbeabsichtigt liegen zu lassen oder ein solches zu stehlen gerade weil sie so designt werden, dass sie möglichst klein und nicht störend sind. Wenn jetzt einem Angreifer ein – vormals authentisiertes – Gerät stehlen kann, sollte es dem neuen Benutzer die Dienste verweigern, ausser er weist sich korrekt aus. So wird verhindert, dass der blosse Besitz eines Tokens ausreicht, um Dienste in Anspruch zu nehmen. Es wird dann nicht mehr ausreichen, nur noch den Schlüssel zum Auto zu besitzen, sondern man benötigt auch noch das explizite Recht, das Auto fahren zu dürfen.

2.5 MITM-Sicher

Ein Angriff wie in Punkt 1.2 aufgeführt sollte detektiert und damit nutzlos gemacht werden können. Damit kann man sicherstellen, dass man auch wirklich mit demjenigen Partner kommuniziert, mit dem man beabsichtigt und die Nachrichtsintegrität sowie die Authentizität der Kommunikationspartner kann damit sichergestellt werden, was für sichere Kommunikation wichtig ist, insbesondere wenn man auf vertrauliche Daten (persönliches Home, Banktransaktionen) zugreifen will.

3. Ortsbasierte Authentifizierung

Bei ortsbasierter Authentifizierung wird, wie der Name schon impliziert, die Ortsinformation zusätzlich zum vorhandenen Sicherheitscheck miteinbezogen. Dies bedeutet, dass zum Beispiel der Besitz des Schlüssel-Tokens ausreicht, aber die Inanspruchnahme eines Dienstes nur an einem bestimmten Punkt oder in einer genau definierten Region überhaupt möglich ist. Das Erzwingen von Aktionen nur in bestimmten Bereichen ermöglicht auch neuartige Dienste, wie zum Beispiel die Freischaltung von vertraulichen Informationen für alle Anwesenden im Sitzungszimmer für ihre Geräte, nicht aber für Leute von ausserhalb oder Zusatzinformationen für die Besucher in einem Stadion oder Museum.
Der administrative Aufwand für so ein System nachdem es aufgebaut wurde ist sehr klein, da der neu zu berücksichtigende Wert binär ist, also ausschliesslich den Aufenthalt im bestimmten Bereich bestätigt oder verneint.
Am Beispiel des Echo-Protokolls von Sastry et al. [6] wird ein solches System vorgestellt.

3.1 Echo Protokoll

Beim Echo-Protokoll werden ein oder mehrere Prüfer (Verifier V) eingesetzt, wobei jeder Prüfer eine bestimmte, typischerweise kreisförmige Region hat, in welcher er mit Bestimmtheit den Aufenthalt eines Prüflings bestätigen kann (ROA – Region of Acceptance, Akzeptanz Zone) Zusätzlich existiert noch eine etwas grössere Region, wo der Prüfer einen Prüfling akzeptieren würde, wenn er keinerlei Verarbeitungszeit benötigen würde, also ohne jegliche Verzögerung auf eine entsprechende Nachricht vom Prüfer antworten könnte. Diese Zone ist auf untenstehender Illustration 2 schraffiert dargestellt.

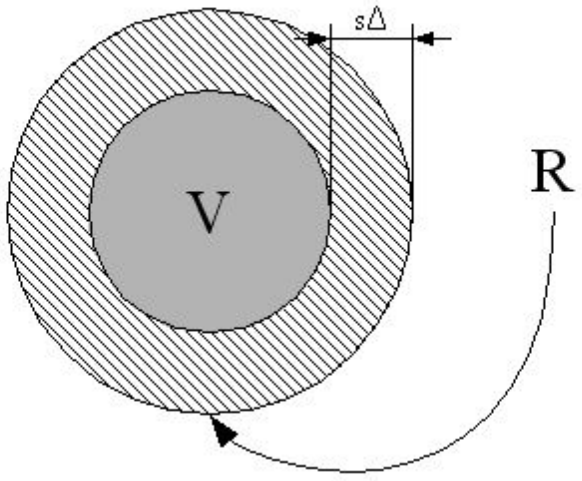

Illustration 2 Prüfer mit Akzeptanz-Zonen

Das Echo-Protokoll verwendet für seine Funktion Funk sowie Ultraschall und benützt eine Laufzeitmessung des Signals, um die Distanz zu bestimmen. Der Ablauf ist wie folgt:

1. Ein Prüfling meldet sich bei einem Prüfer und teilt seinen Abstand zu diesem, sowie seine technisch bedingte maximale Verzögerungszeit mit. Die Position sowohl des Prüflings wie auch des Prüfers muss dabei im voraus bekannt sein.
2. Der Prüfer entscheidet, ob sich der Prüfling überhaupt in seinem Gebiet befindet und ob die maximale Verzögerung des Prüflings ausreicht, um noch akzeptiert zu werden. Trifft dies nicht zu, so verweigert er die Authentifizierung, andernfalls sendet er über Funk eine *nonce (*ein zufälliger Bitstrom) an den Prüfling.
3. Der Prüfling empfängt die nonce und sendet sie sofort über Ultraschall an den Prüfer zurück.
4. Der Prüfer misst die Zeit zwischen Senden und Empfang der nonce und prüft letztere auf Korrektheit. Durch die Zeitdifferenz kann der Prüfer nun entscheiden, ob der Prüfling tatsächlich innerhalb der Region ist oder ob er weiter weg ist und akzeptiert ihn darauf basierend oder nicht.

Da auf dem Rückweg Ultraschall anstelle von Funk eingesetzt wird, ist es einem entfernt stehenden Angreifer enorm erschwert, eine Antwort rechtzeitig zu senden. Da sich Schall viel langsamer als Licht (und Funk) ausbreitet, bedeutet eine Verzögerung von 1/10tel Sekunde bereits einen Distanzunterschied von 30 Metern. Funk hingegen breitet sich mit nahezu Lichtgeschwindigkeit aus, was selbst bei kleinsten Zeitverzögerungen mehrere Kilometer Distanzunterschied ausmachen würde. Auf diese Art und Weise kann relativ kostengünstig eine Distanzmessung vorgenommen werden, die selbst bei Geräten mit geringer CPU-Leistung und suboptimalen Antwortzeiten im einstelligen Millisekundenbereich noch einigermassen genau die Position bestimmen kann.
Die nonce sorgt dafür, dass ein Angreifer nicht schon seine Antwort senden kann, bevor er die Aufforderung dafür erhält. Sie kann also nicht gesendet werden, bevor sie empfangen wurde, was ein Umgehen der Regionsbeschränkung vereitelt.

Um einen Raum abzudecken, benötigt man je nach dem mehrere Prüfer, welche entsprechend genau plaziert werden müssen, damit der Raum, nicht aber die Region ausserhalb akzeptiert wird.

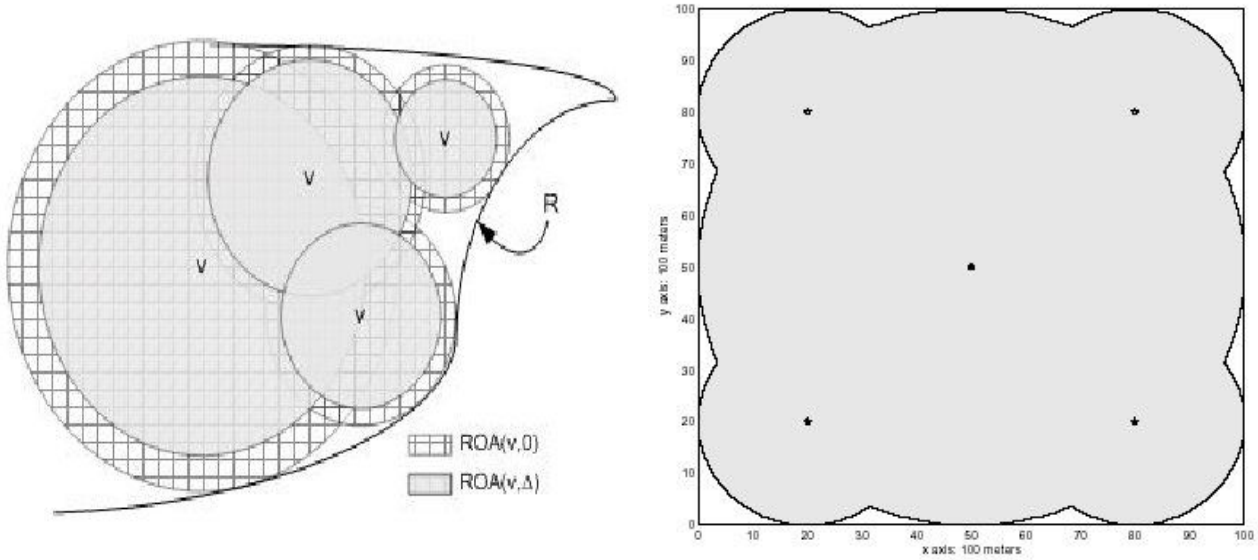

Illustration 3 Raumabdeckung mit mehreren Prüfern

4. Drag and Drop Interaktion

Unter Drag and Drop versteht man das Ziehen eines Objektes mit dem Mauszeiger durch kontinuierliches Drücken der Maustaste sowie das anschliessende „fallenlassens“ dieses Objektes durch das Loslassen der Maustaste. Dieses recht bekannte Paradigma wurde nun von Sastry et al. [7] für die intuitive und sichere Interaktion wiederverwendet.
Als Basis dient ein persönliches Token, in der Illustration als Ring dargestellt. Die „Drag-Aktion“ wird nun durch Berührung des Tokens mit einem Zielobjekt ausgelöst, danach kann innert eines bestimmten Zeitraumes die Drop Aktion durch Berührung eines Zielobjektes ausgelöst werden. Dabei werden nun Daten des ersten Objektes über das Token an das Zielobjekt übermittelt. Als Beispiel wurden Daten von von einer Uhr an den PDA des Benutzers übertragen:

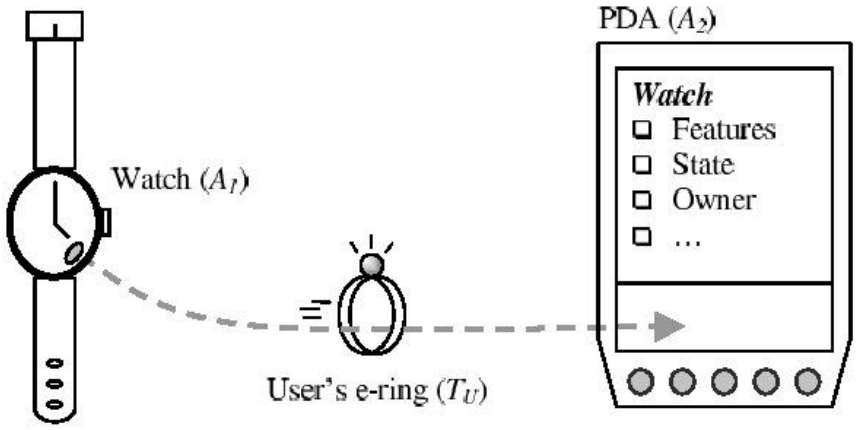

Illustration 4 Drag and Drop der Daten von der Uhr zum PDA

Das persönliche Token des Benutzers kann allerdings auch als Zertifikatsspeicher und damit als digitale Signatur des Benutzers verwendet werden. Dazu genügt ebenfalls ein intuitives Berühren des Tokens mit dem zu signierenden Gegenstand. Damit jetzt aber beim Verlust des Tokens nicht andere Personen dieses verwenden können, erlaubt das Token solche Aktionen erst, nachdem der Besitzer sich am Token authentifiziert hat. Beim Abziehen oder nach einiger Zeit wird es wieder inaktiv und benötigt erneut eine Authentifizierung. Durch dieses Freischalten wird die Benutzung des Tokens einfach und stört nicht im täglichen Gebrauch, kompromittiert aber auch nicht die Sicherheit, sollte es verloren gehen.
Da das Token selber keine richtige Anzeige hat, muss sichergestellt werden, dass die Daten die es transportiert auch wirklich vom entsprechenden Objekt stammen, welches berührt wurde. Dazu verwendet dieses System das sogenannte Distance-Bounding Protokoll welches ausführlich in [7] erklärt wird und grundsätzlich ähnlich wie das in 3.1 vorgestellte Echo Protokoll durch Laufzeitmessung funktioniert, ausser der noch zusätzlich am Ende des Protokolls stattfindende Zertifikatstausch, so dass alle Aktionen auf Wunsch durch Zertifikate beglaubigt werden. Ein alternativer, anonymer Modus steht ebenfalls zur Verfügung, so dass nicht schon beim genaueren Betrachten der Daten eines Objektes bekannt ist, wer die Daten wissen möchte. So kann man sicherstellen, dass das Shopping möglich ist, ohne ein System welches seine Benutzer gezielt verfolgt und auf Schritt und Tritt beobachtet, auch wenn sie schlussendlich nichts kaufen.

5. Fazit

In einer stark vernetzten Welt voller mobiler Geräte wird es zunehmen wichtiger, die Vertraulichkeit und Sicherheit der Daten und die Authentizität der beteiligten Parteien sicher zu stellen, auch wenn sie sich vorher noch nie begegnet sind, da Angriffe sehr einfach aus sicherer Distanz durchgeführt werden können. Da auf der anderen Seite aber auch die Handhabung der Systeme nicht kompliziert und umständlich werden darf, sind einfach zu Verwendende aber dennoch sichere Mechanismen gesucht. Eine mögliche Lösung für dieses Problem stellt die ortsbasierte Authentifizierung dar, welche sicherstellt, dass ein Benutzer oder Gerät auch wirklich dort ist, wo es vorgibt zu sein. Dadurch wird sehr effektiv vermieden, dass ein Angreifer bequem aus der Distanz seinen Angriff durchführen kann und gleichzeitig wird ein legitimer Benutzer nicht durch umständliche Sicherheitsmassnahmen behindert.
Weiterhin ermöglicht die Kenntnis von Ortsinformation neue ortsbezogene Dienste. Das bedeutet dass die Ortsinformation in der mobilen Welt immer wichtiger wird. Da die Ortsbestimmung je nach Genauigkeit mit relativ simplen Protokollen und mittels Zeitmessung möglich ist, kann dies auch mit billigen Geräten durchgeführt werden, was für eine breite Verwendung essentiell ist. Allerdings benötigt man hierzu eine vorhandene Infrastruktur, die natürlich noch nicht existiert und entsprechende Investitionen voraussetzt. Dies dürfte dem Einsatz solcher Systeme vorerst noch die grösste Hürde sein. Weiterhin soll nicht verschwiegen werden, dass auch mittels ortsbezogener Authentifizierung nicht alle Probleme gelöst werden. Ein Angreifer kann durchaus ein von ihm kontrolliertes Gerät in die Zielregion bringen und dann dieses als Proxy verwenden, welches nun Zugriff ermöglicht da es sich ja im erlaubten Bereich befindet.

6. Referenzen

[1] http://wireless.utk.edu/overview.html – Übersicht kabelloser Technologien
[2] http://www.telekom3.de/de-p/aktu/3-ne/2004/06-j/040608-mobilfunk-studie-ar,templateId=_2Fdt_2Fweb_2Fstruct_2FContent.jsp.html - Markstudie Mobiltelefon
[3] http://www.peterindia.net/WearableComputingLinks.html – Wearable Computing
[4] http://en.wikipedia.org/wiki/Man_in_the_middle – Wikipedia Eintrag zur MITM Attacke
[5] Howard Chivers, John A. Clark, and Susan Stepney. *Smart Devices and Software Agents: The Basics of Good Behaviour*. Security in Pervasive Computing 2003, LNCS 2802, pp. 39-52, 2004
[6] Naveen Sastry, Umesh Shankar, David Wagner. *Secure Verification of Location Claims*. ACM 1-58113-769-9/03/0009
[7] Laurent Bussard and Yves Roudier. *Embedding Distance-Bounding Protocols within Intuitive Interactions*. Security in Pervasive Computing 2003, LNCS 2802, pp. 143-156, 2004