



E-Voting-Technologien und Protokolle

Seminar „Security-Protokolle für E-Commerce“

Rene Schneider

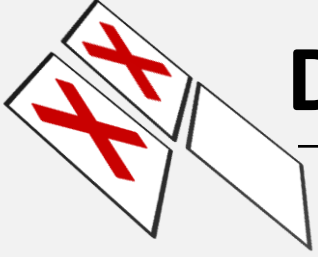
rs034@hdm-stuttgart.de



Agenda

- Die zwei Formen des E-Voting
 - Präsenzwahlen -> Wahlcomputer
 - Distanzwahlen -> Wahlen über das Internet
- Wahlcomputer
 - Überblick über Systeme am Markt
 - Angriffsszenarien und Sicherheitsschwächen
- Internetwahlen
 - Ansprüche an Internet-Wahlsysteme und Angriffsszenarien
 - Grundlagen der heute bekannten E-Voting-Protokolle
- Fazit
 - E-Voting heute: Pro und Contra -> Diskussion

Die zwei Formen des E-Voting

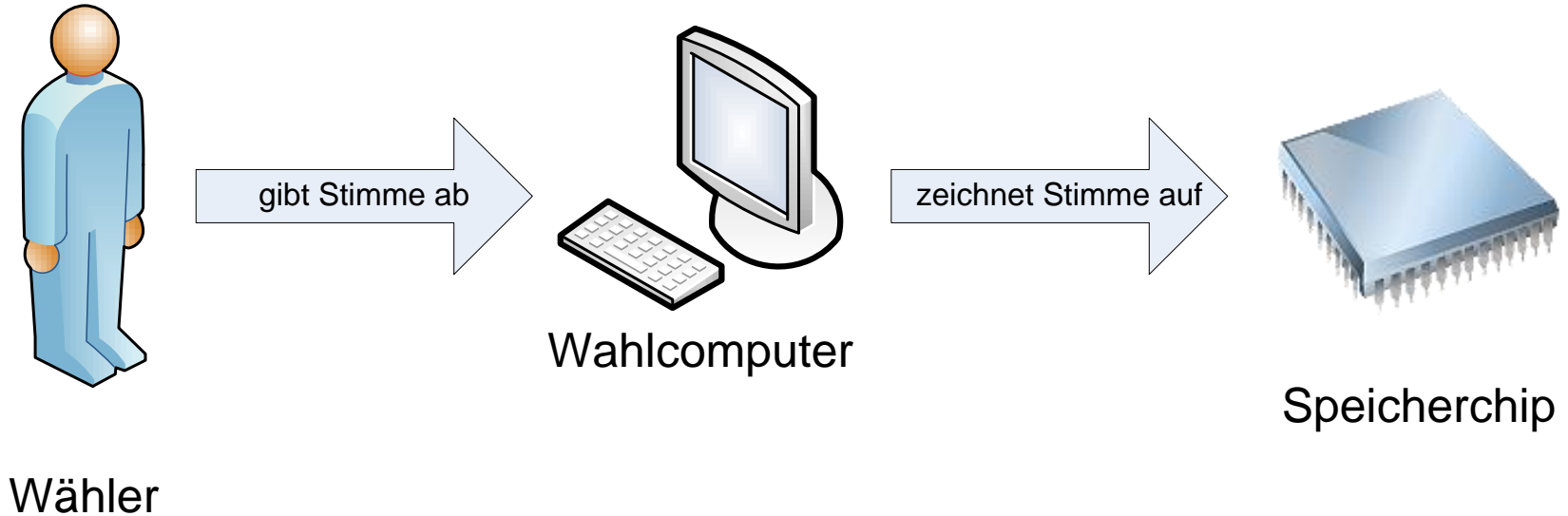


- Grundsätzlich kann bereits bei herkömmlichen Wahlen zwischen zwei Wahlformen unterschieden werden
 - Präsenzwahlen
 - Der Wähler ist persönlich anwesend an einem öffentlichen Wahlort
 - Die Stimme wird unter Beaufsichtigung durch Wahlhelfer und anderen Wählern abgegeben (die Wahlentscheidung des Einzelnen findet natürlich unbeaufsichtigt statt)
 - Distanzwahlen
 - Die Wahl findet „aus der Ferne“ statt, d.h. über Fernkommunikation
 - Die Umstände bei der Abgabe der Stimme sind nicht kontrollierbar
- Auch E-Voting-Systeme lassen sich in diese Kategorien einteilen

Die zwei Formen des E-Voting

Präsenzwahlen

- E-Voting-Alternative: Wahlcomputer
 - werden in klassischen Wahllokalen aufgestellt
 - automatisieren primär den Zählprozess



Wahlcomputer

Marktübersicht

- Marktführer in USA: Election Systems & Software
 - erreicht nach eigenen Angaben 50% aller Wähler



ES&S iVotronic

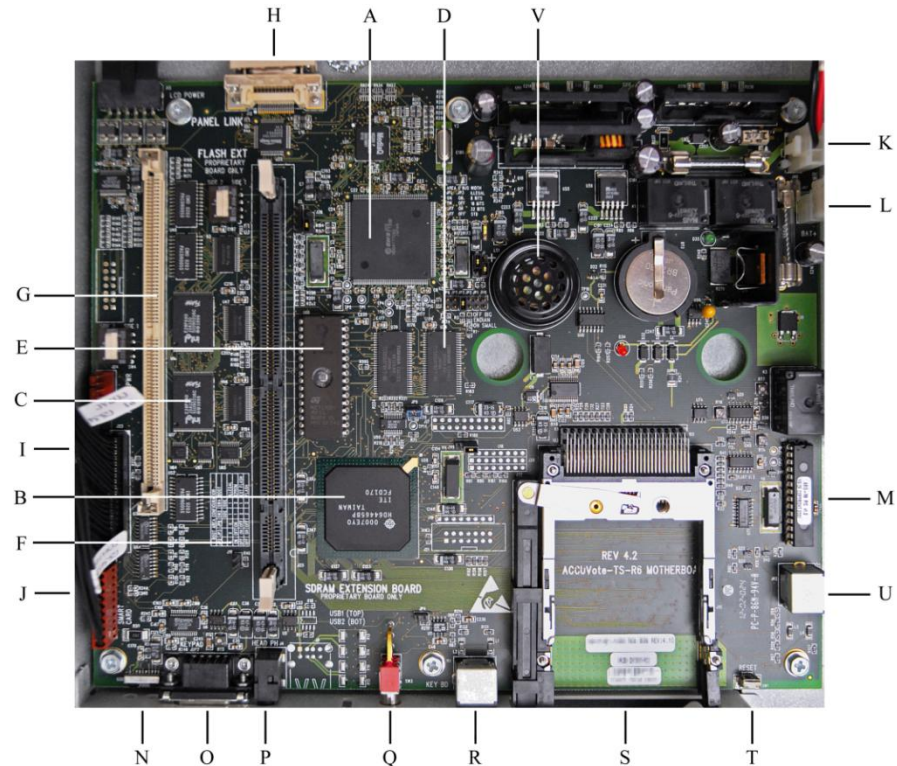
Wahlcomputer

Marktübersicht

- Zweitplatziertes in USA: Premier Election Solutions
 - früher: Diebold Election Systems
 - erreicht gemeinsam mit ES&S 80% aller Wähler



Diebold AccuVote-TS



Wahlcomputer

Marktübersicht

- Marktführer in Europa: Nedap
 - in den Niederlanden: ehemals 90% aller Wähler
 - in Deutschland: mehrere tausend Maschinen



Wahlcomputer

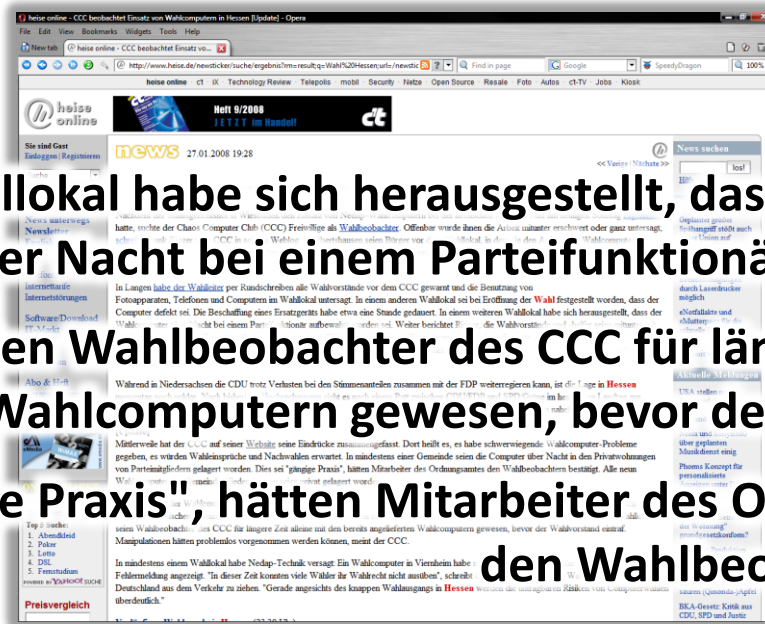
Angriffsszenarien

- Vor der Wahl
 - Manipulation der Wahlcomputer-Software
 - Beim Hersteller / durch offizielle Updates
 - Am Lagerort in der Gemeinde
 - Unmittelbar vor der Wahl im Wahllokal

In einem weiteren Wahllokal habe sich herausgestellt, dass der Wahlcomputer über Nacht bei einem Parteifunktionär aufbewahrt worden sei.

In zwei Wahllokalen seien Wahlbeobachter des CCC für längere Zeit alleine mit den bereits angelieferten Wahlcomputern gewesen, bevor der Wahlvorstand eintraf.

Dies sei "gängige Praxis", hätten Mitarbeiter des Ordnungsamtes den Wahlbeobachtern bestätigt.





Wahlcomputer

Angriffsszenarien

- Während der Wahl
 - Ausnutzen von Unkenntnis und Unsicherheit der Wähler
 - Manipulation einer Wahl in den Niederlanden durch einen Wahlhelfer, der nicht endgültig abgegebene Stimmen „korrigierte“ und selbst abgab
 - Ausspähen von elektromagnetischen Emissionen und Rekonstruktion des Bildschirm/Display-Inhalts



Wahlcomputer

Angriffsszenarien

- Nach der Wahl
 - Manipulation der Wahlmanagement-Software
 - Läuft in der Regel auf normalen Windows-PCs ohne spezielle Sicherheitsvorkehrungen, teilweise mit Internetanbindung sowie veralteten Betriebssystemen (Windows 2000)
 - Manipulation der Ergebnis-Speichermedien vor dem Auslesen

Wahlcomputer

Angriffsszenarien

- Gefährlichstes Szenario: Manipulation der Wahlcomputer-Software vor der Wahl
 - Kann in großem Maßstab durchgeführt werden
 - Durch Manipulation vieler/aller Geräte werden Eingriffe in die Stimmauszählung breit gestreut und damit unauffälliger
 - Mangels Nachzählungsmöglichkeit bei DRE-Geräten ist die Gefahr der Enttarnung durch an der Durchführung der Wahl beteiligte Personen gering
 - Aufwendig bei der Vorbereitung, aber kurze „kritische Phase“
 - Vorbereitung erfordert Fachkenntnisse und Zeit, kann aber „in aller Stille“ durchgeführt werden
 - Das Einbringen der manipulierten Software in die Wahlcomputer ist innerhalb von Minuten und ohne Fachkenntnisse möglich

Wahlcomputer

Sicherheitsmaßnahmen

- Diebold AccuVote-TS
 - einziges Sicherheitsmerkmal am Gerät: verschlossene Blende vor Power-Knopf und Slot für Flash-Speicherkarte
 - Schloss ist nach Aussage in [1] mit mäßigen Kenntnissen im Schlösserknacken innerhalb von 10 Sekunden zu öffnen
 - Zugriff auf Speicherkartenslot ermöglicht Einspielen jeglicher Schadsoftware
 - Beim Booten kann der Bootloader sowie das Betriebssystem-Image über den Update-Prozess der Geräte beliebig ersetzt werden.
 - Keine Öffnung des Geräts notwendig -> keine sichtbaren Spuren
 - Manipulation ist in einer Minute abgeschlossen

[1] Security Analysis of the Diebold AccuVote-TS Voting Machine - Princeton University, 2006
<http://itpolicy.princeton.edu/voting/ts-paper.pdf>



Wahlcomputer

Sicherheitsmaßnahmen

- Diebold AccuVote-TS
 - Manipulation kann sich im Stil eines Virus selbst ausbreiten, indem eine manipulierte Maschine jede eingesteckte Speicherkarte infiziert
 - Mangels VVPAT* und geeigneter Sicherheitsmechanismen in der Software des Geräts kann ein Schadprogramm parallel zur Wahlsoftware laufen und gespeicherte Stimmen beliebig verändern, ohne dass dies auffällt

* Voter-Verified Paper Audit Trail, d.h. ein parallel zur Wahl erstellter Ausdruck der Stimme, der vom Wähler kontrolliert und separat – wie bei Stimmzetteln üblich – in Urnen gesammelt wird.



Wahlcomputer

Sicherheitsmaßnahmen

- Nedap ESD1/ESD2*:
 - Schlösser sollen kritische Aktionen wie das Herausnehmen oder Einsetzen von Speichermodulen und das Freigeben des Computers physikalisch schützen
 - Die Schlüssler sind landesweit identisch und für Cent-Beträge legal zu beziehen (vom deutschen Nedap-Distributor oder anderen Quellen)
 - Die verwendeten Schlösser sind billigster Bauart und werden vom Hersteller für unkritische Anwendungen wie „Büromöbel“ empfohlen

* Diese Bautypen wurden bislang keiner ausführlichen, unabhängigen Sicherheitsanalyse unterzogen, wohl aber der praktisch baugleiche, auf niederländische Wahlen programmierte Typ ES3B



Wahlcomputer

Sicherheitsmaßnahmen

- Nedap ESD1/ESD2*:
 - Eine Checksumme soll dem Wahlvorstand direkt vor der Wahl die Verifikation der Software auf dem Wahlcomputer erlauben
 - Die Checksumme wird von derselben Software berechnet, welche auch die Stimmen zählt
 - Ein Angreifer wird nicht versäumen, die Checksummenberechnung zu patchen, so dass diese stets die erwartete Ausgabe erzeugt

* Diese Bautypen wurden bislang keiner ausführlichen, unabhängigen Sicherheitsanalyse unterzogen, wohl aber der praktisch baugleiche, auf niederländische Wahlen programmierte Typ ES3B

Wahlcomputer

Sicherheitsmaßnahmen

- Nedap ESD1/ESD2*:
 - Siegel auf der Hardware sollen das unbefugte und unbemerkte Öffnen verhindern, welches erforderlich ist, um eine veränderte Software-Version einzusetzen
 - Die Siegel sind normale, mit einem Laserdrucker bedruckte Papieraufkleber -> Abziehen und Wiederaufkleben ist problemlos möglich, ebenso die Fälschung
 - Sie sind lediglich mit einer Seriennummer und einer Unterschrift versehen und besitzen keine weiteren „fälschungssicheren“ Merkmale
 - Sie sind unsichtbar für den Wähler, so dass dieser keine Möglichkeit hat, die Unversehrtheit zu prüfen



* Diese Bautypen wurden bislang keiner ausführlichen, unabhängigen Sicherheitsanalyse unterzogen, wohl aber der praktisch baugleiche, auf niederländische Wahlen programmierte Typ ES3B

Die zwei Formen des E-Voting

Distanzwahlen

- E-Voting-Alternative: Internet-Wahlen
 - Bürger stimmen von einem beliebigen internetfähigen Rechner aus ab
 - Der Aufenthaltsort zum Zeitpunkt der Stimmabgabe ist irrelevant
 - Das Wahlsystem muss möglichst alle Aspekte einer demokratischen Wahl berücksichtigen



Internet-Wahlen

Anforderungen

- Die Anforderungen an ein Internet-Wahlsystem ergeben sich aus den prinzipiellen Anforderungen an eine demokratische Wahl
 - Diese Anforderungen sind je nach Land leicht unterschiedlich angelegt, ähneln sich jedoch in großen Teilen
 - In Deutschland gilt Art. 38 GG: „Die Abgeordneten des Deutschen Bundestages werden in allgemeiner, unmittelbarer, freier, gleicher und geheimer Wahl gewählt.“



Internet-Wahlen

Anforderungen – "...allgemein..."

- Eine Wahl ist allgemein, wenn es allen Staatsbürgern unbedingt zusteht, an ihr teilzunehmen.
 - akzeptierte Ausnahme: Mindestalter
 - Technische Anforderungen an Internet-Wahlsysteme:
 - Ein Internet-Wahlsystem muss von allen gängigen Rechnern aus nutzbar sein
 - Das Wahlsystem muss eine parallel stattfindende Präsenzwahl und/oder papiergebundene Distanzwahl (Briefwahl) sowie die Zusammenführung der Stimmen erlauben



Internet-Wahlen

Anforderungen – "...unmittelbar..."

- Eine Wahl ist unmittelbar, wenn die Stimmen direkt die Zuteilung der Abgeordnetensitze festlegen
 - Legt keine technischen Anforderungen an Internet-Wahlssysteme fest
 - Ist außerdem hochspezifisch für die deutsche Bundestagswahl



Internet-Wahlen

Anforderungen – "...frei..."

- Eine Wahl ist frei, wenn keine Einflussnahme von dritter Seite in den Wahlprozess stattfindet
 - Technische Anforderungen an Internet-Wahlsysteme:
 - Bei der Abgabe der Stimme am Rechner darf keine Einflussnahme durch parallel laufende Programme möglich sein
 - Die Stimmabgabe muss durch die stimmberechtigte Person selbst vorgenommen werden; automatisierte Stimmabgaben dürfen nicht möglich sein
 - Die abgegebene Stimme muss vor Manipulation geschützt übertragen und gespeichert werden
 - Der Wähler darf keinen verlässlichen, dauerhaften Beleg über seine Stimmabgabe erhalten, da ein solcher Stimmenkauf ermöglicht



Internet-Wahlen

Anforderungen – "...gleich..."

- Eine Wahl ist gleich, wenn jeder Wähler dieselbe Anzahl Stimmen mit jeweils gleichem Gewicht hat.
 - Technische Anforderungen an Internet-Wahlsysteme:
 - Die gleichzeitige Stimmabgabe durch Internetwahl und Präsenzwahl darf nicht möglich sein
 - Mehrfache Stimmabgaben durch eine Person im Internet-Wahlsystem müssen unterbunden werden

Internet-Wahlen

Anforderungen – "...geheim..."

- Eine Wahl ist geheim, wenn der Wähler seine Stimme unbeobachtet abgibt und auch im Nachhinein nicht feststellbar ist, wie eine einzelne Person gewählt hat
 - Technische Anforderungen an Internet-Wahlsysteme:
 - Die Stimme des Wählers muss auf anonyme Weise gespeichert werden
 - So lange eine Zuordnung einer digitalen Stimme zu einem Wähler möglich ist (z.B. während der Übertragung), darf die Stimme für niemanden einsehbar sein



Internet-Wahlen

Anforderungen - Transparenzgebot

- Zusätzliche Anforderungen ergeben sich aus dem Transparenzgebot, welches für alle demokratischen Wahlen gilt
- Eine Wahl ist transparent, wenn das Wahlsystem offen bekannt und eine Beobachtung des Wahl- und Auszählungsprozesses durch jedermann möglich ist.
 - Technische Anforderungen an Internet-Wahlsysteme:
 - Die Funktionsweise des Wahlsystems und sämtliche beteiligten Komponenten müssen offengelegt werden; eine solche Offenlegung darf die Integrität des Systems nicht beschädigen
 - Eine Kontrolle der mit der technischen Durchführung der Wahl betrauten Instanz muss während der gesamten Wahl möglich sein

Internet-Wahlen

Anforderungen - Zusammenfassung

- Die Anforderungen an ein Internet-Wahlsystem sind breit gefächert und widersprechen sich teilweise
 - Die Stimme muss anonym und manipulationssicher übertragen und gespeichert werden, gleichzeitig muss diese aber zählbar sein und es muss festgestellt werden können, ob ein Wähler bereits eine Stimme abgegeben hat
 - Der Wähler darf keinen Beleg über seine Wahlentscheidung erhalten, gleichzeitig muss er sich aber davon überzeugen können, dass seine Stimme korrekt gezählt wurde
 - Das Wahlsystem und der Wahlprozess müssen für den Wähler offen einsehbar sein, gleichzeitig ist für die Realisierung eines Internet-Wahlsystems komplexe IT-Technik nötig

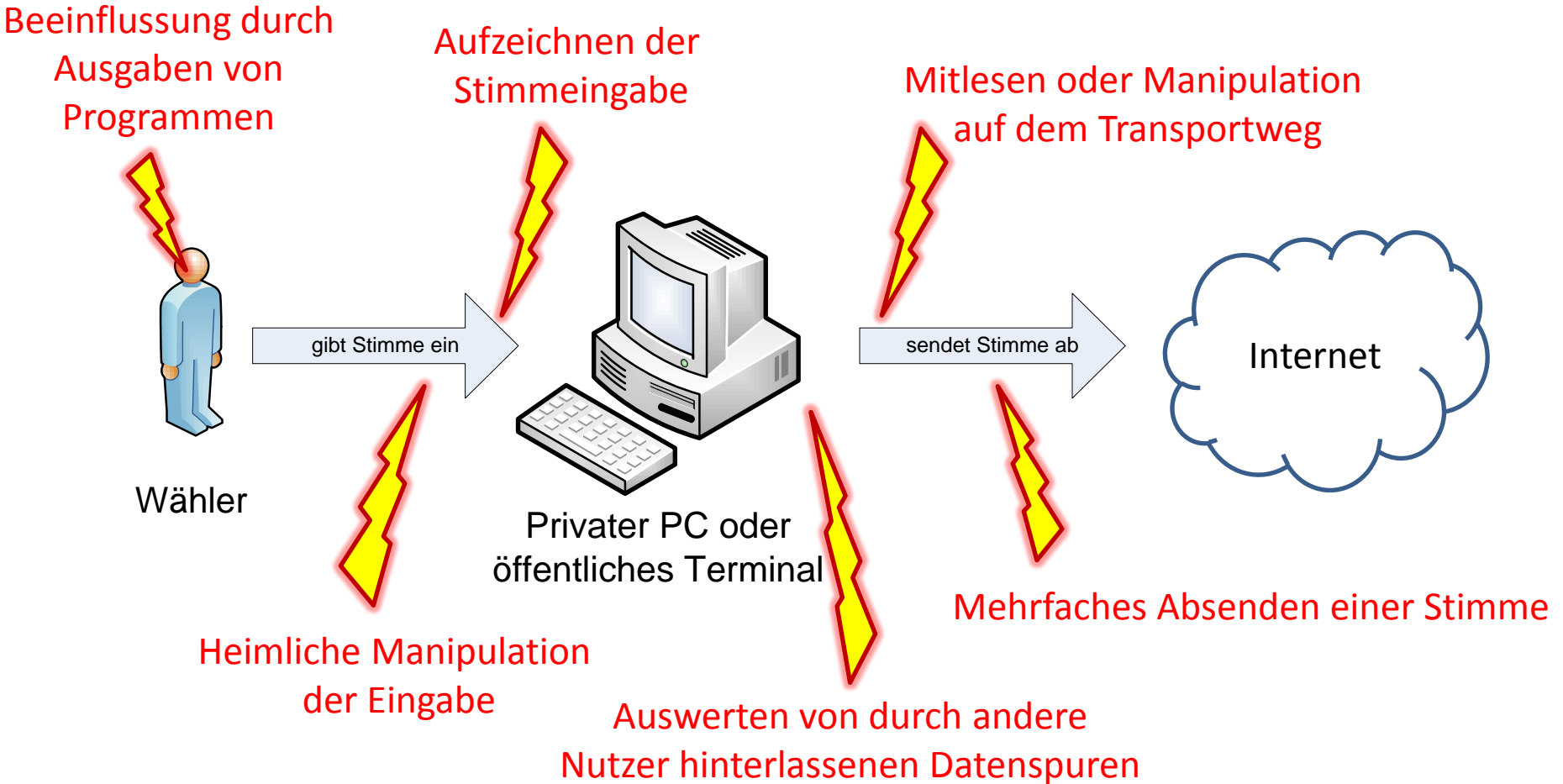
Internet-Wahlen

Angriffsszenarien

- Um die Tauglichkeit von Mechanismen, welche die Erfüllung der aufgestellten Anforderungen sicherstellen sollen, beurteilen zu können, ist zunächst eine Identifikation der potentiellen Angriffspunkte erforderlich.

Internet-Wahlen

Angriffsszenarien

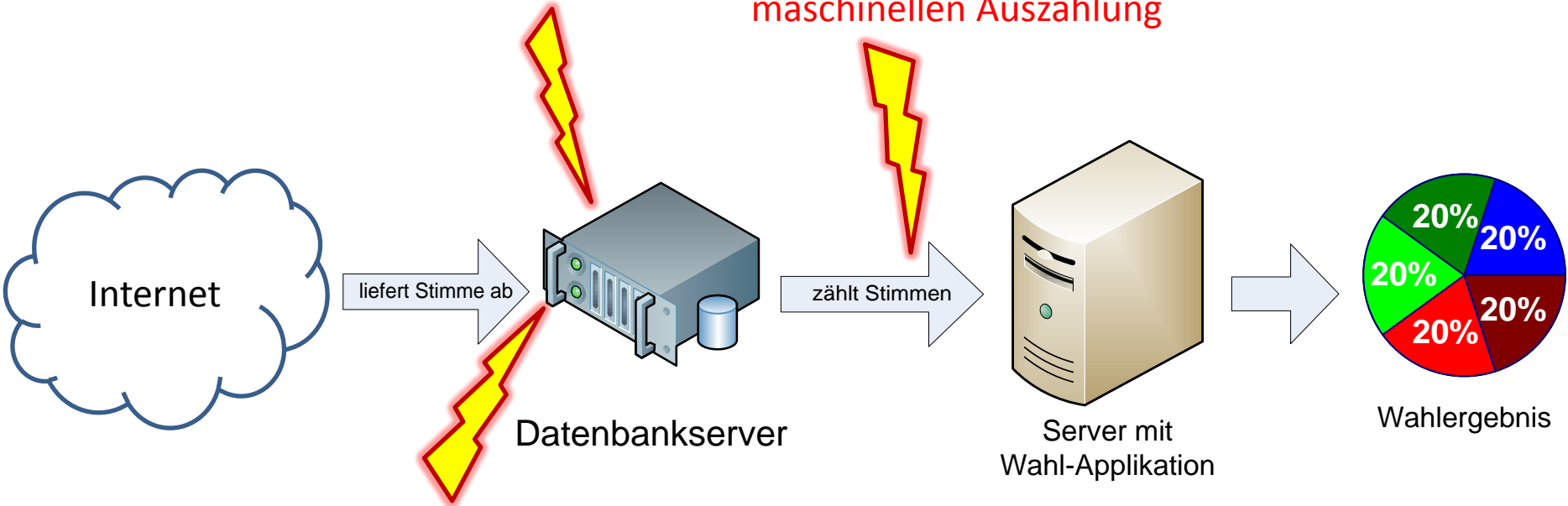


Internet-Wahlen

Angriffsszenarien

Veränderung/Löschung/Einschleusung
von Stimmen durch Innetäter

Manipulation der
maschinellen Auszählung



Verknüpfung von Stimmen
mit einem konkreten Wähler



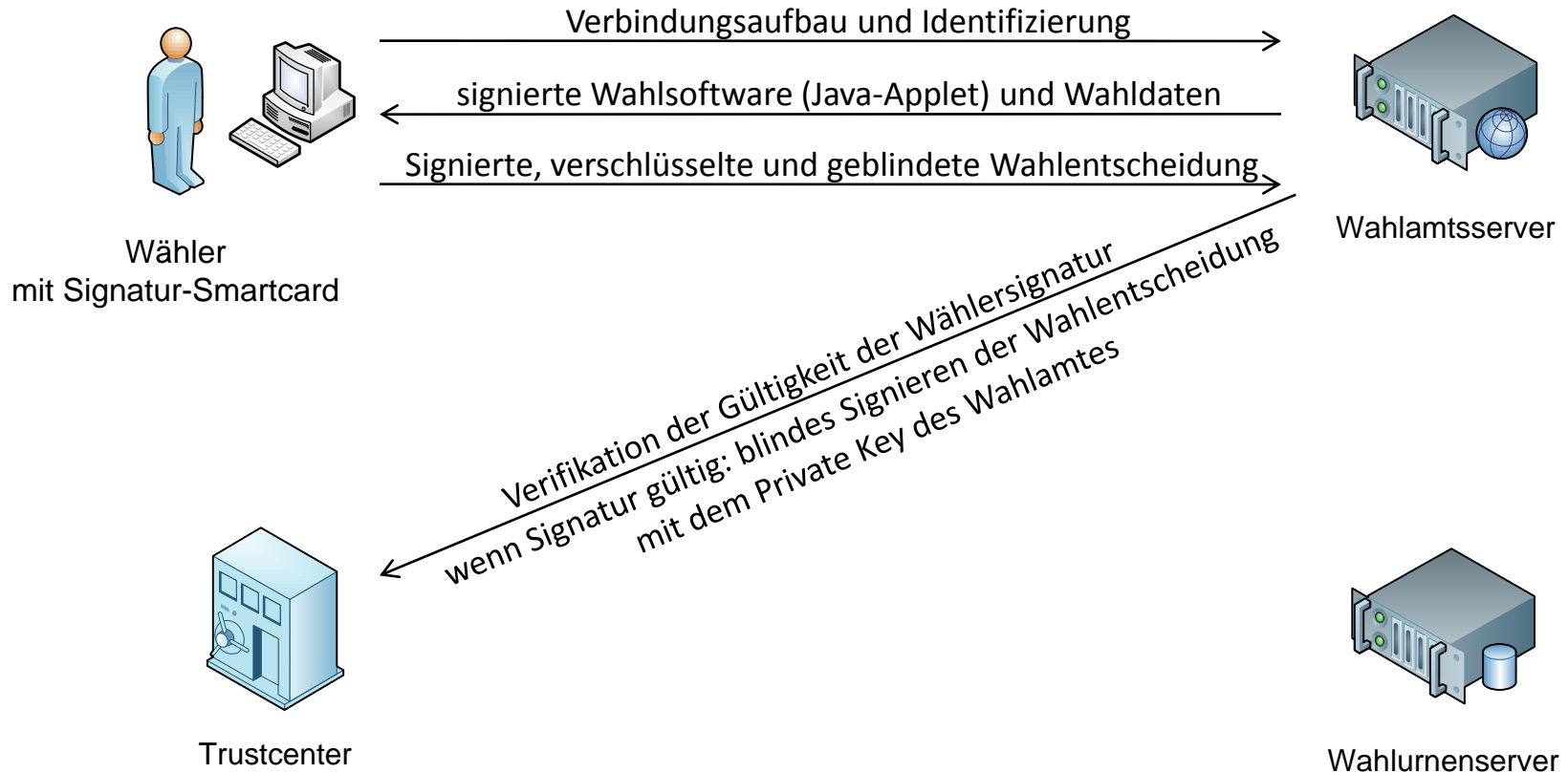
Internet-Wahlen

E-Voting-Systeme

- Grundsätzlich existieren sehr viele Ansätze zu E-Voting-Systemen, welche die aufgestellten Anforderungen unterschiedlich gut erfüllen
- **Kein derzeit bekanntes Protokoll bzw. System erfüllt alle Anforderungen vollständig!**
- Im Folgenden wird exemplarisch ein von der Forschungsgruppe Internetwahlen an der Universität Osnabrück entwickeltes System vorgestellt, welches versucht, viele Anforderungen abzudecken

Internet-Wahlen

E-Voting-Systeme – "i-vote"



Internet-Wahlen

Grundlagen: Blinde Signatur

- Ausgangssituation: Nachricht m von Alice soll durch Bob mit öffentl. Schlüssel (e, n) und geheimem Schlüssel d blind signiert werden

- Alice bestimmt einen Zufallswert r , so dass

$$\text{ggT}(r, n) = 1$$

und bildet

$$t = r^e m \bmod n$$

- Alice lässt t von Bob signieren und erhält

$$t^d = r^{ed} m^d \bmod n = r m^d \bmod n$$

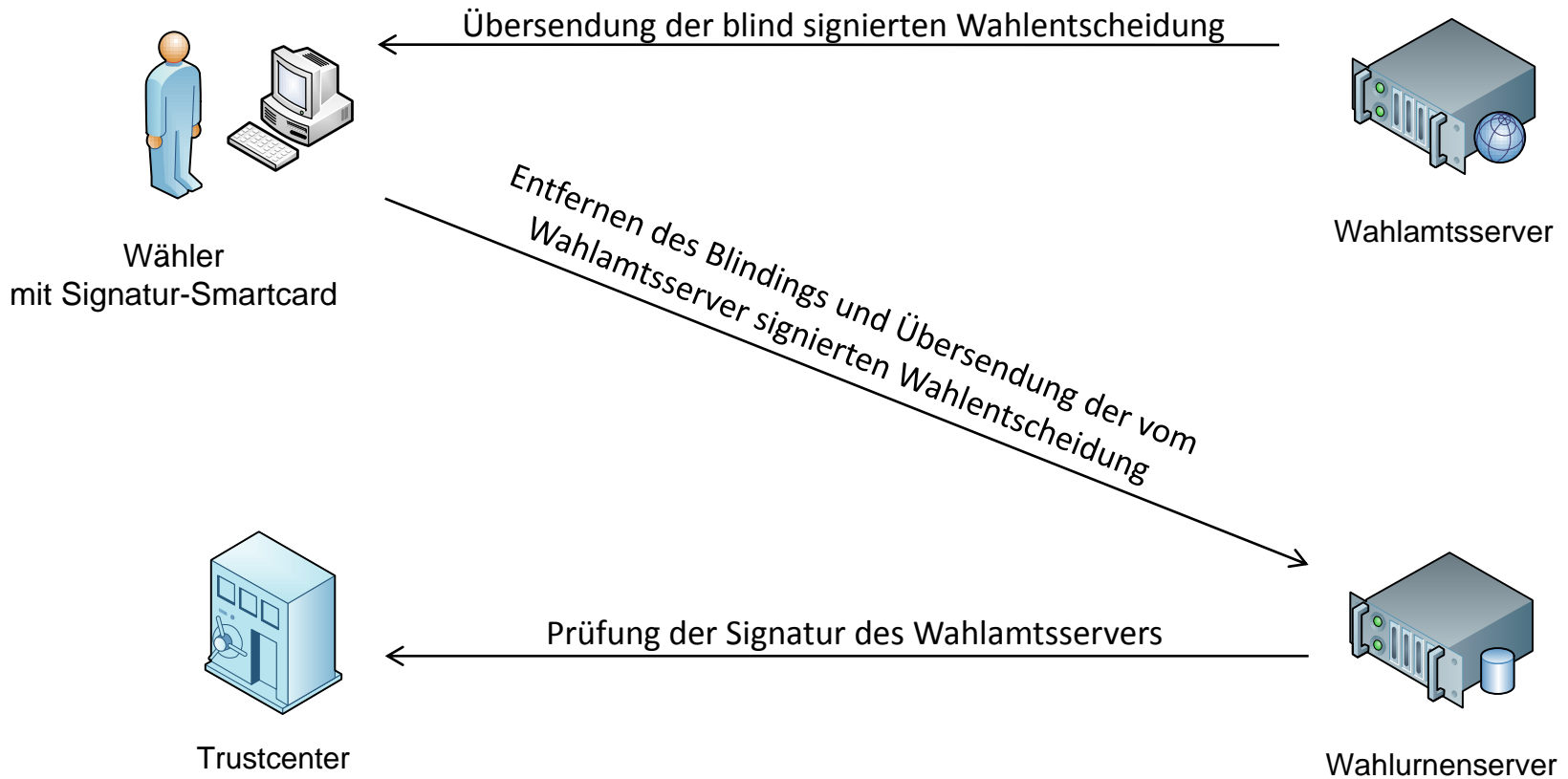
- Alice entfernt den nur ihr bekannten „Blinding Factor“ und erhält die mit d signierte Nachricht:

$$r^{-1} t^d \bmod n = m^d \bmod n$$



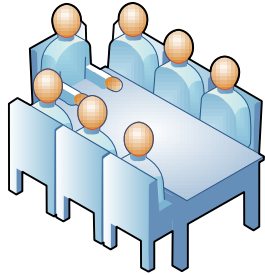
Internet-Wahlen

E-Voting-Systeme – "i-vote"

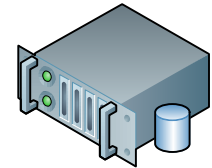
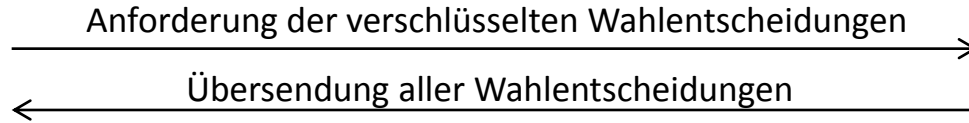


Internet-Wahlen

E-Voting-Systeme – "i-vote"

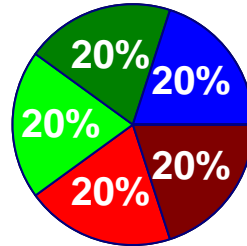
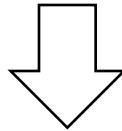


Wahlvorstand



Wahlurnenserver

Anschließend Entschlüsselung mit Private Key des Wahlvorstands
und Auszählung der Wahlentscheidungen



Wahlergebnis



Internet-Wahlen

E-Voting-Systeme – "i-vote"

- Vorteile:
 - Durch räumliche, technische und administrative Trennung von Wahlamts- und Urnenserver wird die Manipulation durch Innentäter erschwert
 - Blinde Signatur durch Wahlamtsserver anonymisiert die eigentliche Stimmenabgabe, erlaubt aber trotzdem eine Pflege von Wählerlisten und damit die Verhinderung einer doppelten oder unberechtigten Stimmabgabe
 - Verschlüsselung verhindert effektiv das Ausspähen von Wahlentscheidungen

Internet-Wahlen

E-Voting-Systeme – "i-vote"

- Nachteile:
 - Es gibt keine universelle Verifizierbarkeit des Wahlergebnisses (d.h. Dritte können das Ergebnis nicht mathematisch prüfen)
 - Wenn der Rechner des Wählers nach der Übersendung an den Wahlamtsserver, aber vor der Stimmabgabe an den Urnenserver abstürzt, geht die Wahlentscheidung unwiederbringlich verloren
 - Eine Möglichkeit, seine Wahl zu revidieren bzw. zu wiederholen, ist nicht realisierbar, ohne die Anonymität der gespeicherten Stimmen aufzugeben
 - Manipulation auf dem Rechner des Wählers ist möglich, es sei denn es wird der Einsatz einer Boot-CD vorausgesetzt
 - Boot-CD bringt Komfortverlust und Kompatibilitätsprobleme mit sich

Internet-Wahlen

E-Voting-Systeme

- Außerdem hat jedes denkbare Internet-basierte Wahlsystem prinzipbedingte Nachteile
 - Die Wahl findet nicht mehr in kontrollierter Umgebung (-> Wahllokal) statt, was sowohl Beeinflussung als auch Stimmenkauf ermöglicht bzw. begünstigt
 - Durch die hohe Komplexität und das Ausführen kritischer, für den Wahlausgang entscheidender Prozesse auf „undurchsichtigen“ Computern ist eine durchgängige Beobachtung des Wahlprozesses durch Wahlbeobachter nicht mehr möglich



Internet-Wahlen

E-Voting-Systeme - Fazit

- Es ist durchaus möglich, viele der für eine Wahl wichtigen Anforderungen mit einem internetbasierten Wahlsystem zu erfüllen
- Allerdings existiert derzeit kein System, welches alle Anforderungen erfüllt
- Einige prinzipbedingte Nachteile können durch kein denkbare Internet-Wahlsystem aus der Welt geräumt werden
- **Daher: Internet-Wahlen als Ersatz für Briefwahlen denkbar, aber niemals als Ersatz für Präsenzwahlen**